



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hiroshi ISOZAKI, et al.

GAU:

SERIAL NO: 10/729,964

EXAMINER:

FILED: December 9, 2003

FOR: CONTENTS TRANSMISSION/RECEPTION SCHEME WITH FUNCTION FOR LIMITING RECIPIENTS

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number _____, filed _____, is claimed pursuant to the provisions of **35 U.S.C. §120**.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**:
Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2002-357168	December 9, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. _____ filed _____
- ☐ were submitted to the International Bureau in PCT Application Number _____
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. _____ filed _____; and
- ☐ (B) Application Serial No.(s) _____
☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak

Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26, 803

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

10/729,964

T 654

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 2 月 9 日
Date of Application:

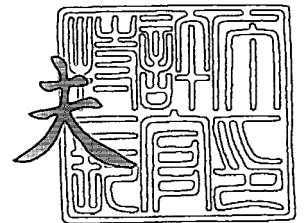
出 願 番 号 特 願 2 0 0 2 - 3 5 7 1 6 8
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 3 5 7 1 6 8]

出 願 人 株式会社東芝
Applicant(s):

2 0 0 3 年 7 月 1 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 5 7 4 4 6

【書類名】 特許願

【整理番号】 14003301

【提出日】 平成14年12月 9日

【あて先】 特許庁長官殿

【国際特許分類】 H04B 7/26

【発明の名称】 コンテンツ送受信システム、コンテンツ送信装置、コンテンツ受信装置及びコンテンツ送受信方法

【請求項の数】 21

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝
 研究開発センター内

 【氏名】 磯 崎 宏

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝
 研究開発センター内

 【氏名】 石 原 丈 士

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝
 研究開発センター内

 【氏名】 小 堺 康 之

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝
 研究開発センター内

 【氏名】 斉 藤 健

【特許出願人】

 【識別番号】 000003078

 【住所又は居所】 東京都港区芝浦一丁目1番1号

 【氏名又は名称】 株式会社 東 芝

【代理人】

【識別番号】 100075812

【弁理士】

【氏名又は名称】 吉 武 賢 次

【選任した代理人】

【識別番号】 100088889

【弁理士】

【氏名又は名称】 橋 谷 英 俊

【選任した代理人】

【識別番号】 100082991

【弁理士】

【氏名又は名称】 佐 藤 泰 和

【選任した代理人】

【識別番号】 100096921

【弁理士】

【氏名又は名称】 吉 元 弘

【選任した代理人】

【識別番号】 100103263

【弁理士】

【氏名又は名称】 川 崎 康

【先の出願に基づく優先権主張】

【出願番号】 特願2002-313300

【出願日】 平成14年10月28日

【手数料の表示】

【予納台帳番号】 087654

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0102514

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ送受信システム、コンテンツ送信装置、コンテンツ受信装置及びコンテンツ送受信方法

【特許請求の範囲】

【請求項 1】

送信装置と、この送信装置からコンテンツを受信する少なくとも 1 台の受信装置と、を備えたコンテンツ送受信システムにおいて、

前記送信装置は、

コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う第 1 の認証・鍵交換処理手段と、

前記受信装置の機器識別情報を送信するよう前記受信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、

前記受信装置の IP (Internet Protocol) アドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と前記機器識別情報登録手段に登録されている機器識別情報とが一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求を行った前記受信装置へのコンテンツの配布条件を変更する配布条件決定手段と、を有し

前記受信装置は、

前記送信装置に対して前記コンテンツ送信要求を行うコンテンツ送信要求手段と、

前記送信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報を前記送信装置に送信する機器識別情報送信手段と、を有することを特徴とするコンテンツ送受信システム。

【請求項 2】

前記機器識別情報は、ネットワークインタフェースのMACアドレスであり、
前記機器識別情報検索手段は、前記受信装置のIPアドレスをキーとするMACアドレス検索要求を、前記受信装置が接続されるイーサネット（登録商標）セグメントに送信するとともに、MACアドレス検索結果を受信することを特徴とする請求項1に記載のコンテンツ送受信システム。

【請求項3】

前記機器識別情報検索手段は、ARPにより、前記受信装置のIPアドレスから対応するMACアドレスを検索することを特徴とする請求項2に記載のコンテンツ送受信システム。

【請求項4】

前記第1の認証・鍵交換処理手段は、DTCP (Digital Transmission Contents Protection) による認証・鍵交換処理を行うことを特徴とする請求項1及至3のいずれかに記載のコンテンツ送受信システム。

【請求項5】

前記機器識別情報送信手段は、MACアドレスに電子署名を添付して前記送信装置に送信することを特徴とする請求項3または4に記載のコンテンツ送受信システム。

【請求項6】

前記送信装置は、MACアドレスに電子署名が添付されている場合には、当該MACアドレスが改ざんされているか否かを検証する検証手段を有し、

前記機器識別情報登録手段は、前記検証手段により改ざんされていないと判断された場合のみ、当該MACアドレスを登録することを特徴とする請求項5に記載のコンテンツ送受信システム。

【請求項7】

前記受信装置は、

前記送信装置との間で認証・鍵交換処理を行う第2の認証・鍵交換処理手段と

前記送信装置から暗号化されたコンテンツを受信するネットワークインタフェース手段と、

前記受信された暗号化されたコンテンツを、前記第2の認証・鍵交換処理手段で交換された鍵を用いて復号を行う暗号処理手段と、を有することを特徴とする請求項1及至6のいずれかに記載のコンテンツ送受信システム。

【請求項8】

少なくとも1台の受信装置に対してコンテンツを送信するコンテンツ送信装置において、

コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、

前記受信装置の機器識別情報を送信するよう前記受信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、

前記受信装置のIPアドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求を行った前記受信装置へのコンテンツの配布条件を変更する配布条件決定手段と、を備えることを特徴とするコンテンツ送信装置。

【請求項9】

送信装置からのコンテンツを受信するコンテンツ受信装置において、

前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、

コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、

前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接

続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を備えることを特徴とするコンテンツ受信装置。

【請求項 10】

送信装置と、この送信装置からコンテンツを受信する少なくとも 1 台の受信装置と、を備えたコンテンツ送受信システムにおいて、

前記受信装置は、

前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、

コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う第 1 の認証・鍵交換処理手段と、

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、

前記送信装置の IP アドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を有し

前記送信装置は、

前記受信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報を前記受信装置に送信する機器識別情報送信手段と、

コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う第 2 の認証・鍵交換処理手段と、

前記配布条件決定手段で決定された配布条件に従って、コンテンツの送信制御を行うコンテンツ送信制御手段と、を有することを特徴とするコンテンツ送受信システム。

【請求項 11】

送信装置からのコンテンツを受信可能なコンテンツ受信装置において、

前記送信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、

前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記送信装置からのコンテンツの受信を禁止するコンテンツ受信制御手段と、を備えることを特徴とするコンテンツ受信装置。

【請求項 12】

前記送信装置から自装置の機器識別情報の送信要求があった場合に、前記機器識別情報及び機器識別情報の検索事前通知応答を前記送信装置に送信する自装置情報送信手段を備えることを特徴とする請求項 11 に記載のコンテンツ受信装置。

【請求項 13】

少なくとも 1 台の受信装置に対してコンテンツを送信可能なコンテンツ送信装置において、

前記受信装置に対して、該受信装置の機器識別情報検索を事前通知する事前通知手段と、

前記受信装置の IP アドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、

前記機器識別情報検索手段で検索された機器識別情報と、前記機器識別情報登録手段に登録された機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記受信装置から送信された、前記機器識別情報検索の事前通知に対する応答を受信したか否かを判定する要求応答受信判定手段と、

前記比較判定手段及び前記要求応答受信判定手段による判定結果に基づいて、前記受信装置へのコンテンツの配布条件を決定する配布条件決定手段と、を備えることを特徴とするコンテンツ送信装置。

【請求項 14】

送信装置と、この送信装置からコンテンツを受信する少なくとも 1 台の受信装置と、を備えたコンテンツ送受信システムにおいて、

前記送信装置は、

前記受信装置に対して、該受信装置の機器識別情報検索を事前通知する事前通知手段と、

前記受信装置の IP アドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、

前記機器識別情報検索手段で検索された機器識別情報と、前記機器識別情報登録手段に登録された機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記機器識別情報検索の事前通知に対する応答を受信したか否かを判定する要求応答受信判定手段と、

前記比較判定手段及び前記要求応答受信判定手段による判定結果に基づいて、前記受信装置へのコンテンツの配布条件を決定する配布条件決定手段と、を有し

前記受信装置は、

前記送信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報及び機器識別情報の検索事前通知応答を前記送信装置に送信する自装置情報送信手段を有することを特徴とするコンテンツ送受信システム。

【請求項 15】

少なくとも 1 台の受信装置に対してコンテンツを送信可能なコンテンツ送信装置において、

前記受信装置から自装置の機器識別情報検索要求があったか否かを判定する機

器識別情報検索判定手段と、

前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記受信装置へのコンテンツの送信を禁止するコンテンツ送信制御手段と、を備えることを特徴とするコンテンツ送信装置。

【請求項 16】

送信装置からのコンテンツを受信するコンテンツ受信装置において、

前記送信装置に対して、該送信装置の機器識別情報検索を事前通知する事前通知手段と、

前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、

前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を備えることを特徴とするコンテンツ受信装置。

【請求項 17】

送信装置と、この送信装置からコンテンツを受信する少なくとも 1 台の受信装置と、を備えたコンテンツ送受信システムにおいて、

前記送信装置は、

前記受信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、

前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと

判定された場合には、前記受信装置へのコンテンツの送信を禁止するコンテンツ送信制御手段と、を有し、

前記受信装置は、

前記送信装置に対して、該送信装置の機器識別情報検索を事前通知する事前通知手段と、

前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、
コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う
認証・鍵交換処理手段と、

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、

前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、

前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を有することを特徴とするコンテンツ送受信システム。

【請求項18】

送信装置と、この送信装置からコンテンツを受信する少なくとも1台の受信装置と、を備えたコンテンツ送受信方法において、

前記送信装置は、

コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行い

前記受信装置の機器識別情報を送信するよう前記受信装置に対して機器識別情報要求を送信し、

前記受信装置から送信された前記機器識別情報を機器識別情報登録テーブルに登録し、

前記受信装置のIP (Internet Protocol) アドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索し、

前記検索された機器識別情報と前記機器識別情報登録テーブルに登録されている機器識別情報とが一致するか否かを判定し、

一致するか否かの判定結果に応じて、コンテンツ送信要求を行った前記受信装置へのコンテンツの配布条件を変更し、

前記受信装置は、

前記送信装置に対して前記コンテンツ送信要求を行い、

前記送信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報を前記送信装置に送信することを特徴とするコンテンツ送受信方法。

【請求項 19】

送信装置と、この送信装置からコンテンツを受信する少なくとも1台の受信装置と、を備えたコンテンツ送受信方法において、

前記受信装置は、

前記送信装置に対してコンテンツ送信要求を行い、

コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行い、

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信し、

前記送信装置から送信された前記送信装置の機器識別情報を機器識別情報登録テーブルに登録し、

前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索し、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定し、

一致するか否かの判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定し、

前記送信装置は、

前記受信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識

別情報を前記受信装置に送信し、

コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行い

、
前記決定された配布条件に従って、コンテンツの送信制御を行うことを特徴とするコンテンツ送受信方法。

【請求項 2 0】

送信装置と、この送信装置からコンテンツを受信する少なくとも 1 台の受信装置と、を備えたコンテンツ送受信システムにおいて、

前記送信装置は、

前記受信装置に対して、該受信装置の機器識別情報検索を事前通知する事前通知手段と、

前記受信装置の IP アドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、

前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、

前記機器識別情報検索手段で検索された機器識別情報と、前記機器識別情報登録手段に登録された機器識別情報と、が一致するか否かを判定する比較判定手段と、

前記比較判定手段及び前記要求応答受信判定手段による判定結果に基づいて、前記受信装置へのコンテンツの配布条件を決定する配布条件決定手段と、を有し

、
前記受信装置は、

前記送信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、

前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記送信装置からのコンテンツの受信を禁止するコンテンツ受信制御手段と、を有することを特徴とするコンテンツ送受信方法。

【請求項 2 1】

送信装置と、この送信装置からコンテンツを受信する少なくとも 1 台の受信装

置と、を備えたコンテンツ送受信方法において、

前記送信装置は、

前記受信装置から自装置の機器識別情報検索要求があったか否かを判定し、

前記機器識別情報検索要求がなかったと判定された場合には、前記受信装置へのコンテンツの送信を禁止し、

前記受信装置は、

前記送信装置に対して、該送信装置の機器識別情報検索を事前通知し、

前記送信装置に対してコンテンツ送信要求を行い、

コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行い

前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信し、

前記送信装置から送信された前記送信装置の機器識別情報を登録し、

前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索し、

前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定し、

一致するか否かの判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定することを特徴とするコンテンツ送受信方法

。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、送信装置から受信装置にコンテンツを送信するコンテンツ送受信システム、コンテンツを送信するコンテンツ送受信システム、コンテンツ送信装置、コンテンツ受信装置及びコンテンツ送受信方法に関する。

【0002】

【従来の技術】

近年の計算機ネットワークの普及やデジタル化に伴い、デジタル情報家電と呼

ばれる製品が普及しつつある。また、地上波デジタル放送の開始に伴い、デジタル放送対応のテレビ、セットトップボックス及びDVDレコーダ等が、今後より一層普及することが予想される。これらのデジタル家電がネットワークで接続されれば利用者にとって有益である。

【0003】

このようなデジタルコンテンツは、劣化することなく容易に複製できるという利点を持つ反面、コンテンツの著作権に関して注意を払わなければならない。

【0004】

図33は送信装置と受信装置を備えた従来のネットワークシステムの全体構成を示すブロック図である。図33に示すように、本発明に係る送信装置1（以下ソース機器Bと呼ぶ）は、イーサネット等のローカルエリアネットワーク2に接続されている。このローカルエリアネットワーク2のイーサネットセグメントA3には、ソース機器B1、受信装置4（以下シンク機器Aと呼ぶ）及びルーター機器C5が接続されている。ルーター機器C5には、インターネット6を介してシンク機器D7が接続されている。シンク機器A4は、ソース機器B1からローカルエリアネットワーク2を経由してコンテンツを受信する。一方、シンク機器D7は、ルーター機器C5とインターネット6を経由してソース機器B1と通信可能な範囲に位置する。

【0005】

ここで、コンテンツとは、例えばMPEG4データのような動画データや音声データ、またはテキストデータや画像データのようなドキュメントなどのデジタルコンテンツを指す。ここでは、説明を簡単にするため、著作権保護をかけた上で転送すべきデジタルコンテンツ（以下、単にコンテンツと呼ぶ）を念頭に置く。

【0006】

ここで、ソース機器B1からシンク機器A4とシンク機器D7にコンテンツを送信する場合を考える。この時、注意すべきはコンテンツの著作権である。前述したように、当該コンテンツをやり取りする範囲は、一定の範囲内、例えば、著作権30条の私的使用の範囲内などの正当な権限の範囲内、あるいはそれよりもさらに狭い範囲内に制限され、その範囲を超えて、例えば他人間でのコンテンツ

のやりとりはできないようにすることが望ましい。

【0007】

そこで、著作権保護を行うために、図33のネットワークシステムにおけるコンテンツの転送に関し、次の規則を用いることとする。

【0008】

(1) ローカルエリアネットワーク内では、著作権保護を行うべきコンテンツの送受信を許可する。なぜならば、ローカルエリアネットワークに接続された機器であれば、個人や家庭内で楽しむ範囲での通信であるとみなすことができるからである。

【0009】

(2) ローカルエリアネットワーク外では、著作権保護を行うべきコンテンツの送受信を許可しない。ローカルエリアネットワーク外での通信とは、例えば図33に示すソース機器B1とシンク機器D7との通信など、インターネットや電話網等の公衆網を介したオープンな通信を示す。なぜならば、ローカルエリアネットワークに閉じない通信は、個人あるいは家庭内で楽しむ範囲の通信とみなすことができないからである。

【0010】

なお、以下では、一例としてローカルエリアネットワークとしてイーサネットを用い、上位レイヤーでのコンテンツの送受信にIP (Internet Protocol) を用いるものとする。IPについては、例えば<http://www.ietf.org>にて取得可能な文献に詳しく記載されている。もちろん、その他のプロトコル、例えばローカルエリアネットワークがIEEE1394で構成されており、上位レイヤーとしてIPをエミュレーションしたIP over 1394であってもよい。

【0011】

コンテンツの配布範囲を個人が楽しむ範囲内に限定するための1つの方法として、同一イーサネットセグメント内に限定した通信のみに許可する方法が考えられる。これを実現するため、従来では、例えば、(1) イーサネットパケットでAKEを行う方法 (特許文献1 参照)、(2) 送受信の機器のネットワークアドレスが同一であるか確認する方法 (特許文献2 参照) などが提案されている。他に

も、(3) TTL (Time To Field) を 1 にセットして IP パケットを送信する方法、
(4) それらを組み合わせた方法などがある。

【0012】

図 34 で示した環境において、ソース機器 B1 からシンク機器へのコンテンツの送受信を同一イーサネットセグメント間に限定するために、(2) と (3) の方法を組み合わせた方法を一例として以下に示す。

【0013】

一般的には、IP において、複数の機器のネットワークアドレスが同一であれば、同一のイーサネットセグメントに所属すると考えられるため、ソース機器 B1 とシンク機器のネットワークアドレスが同一であることを確認すれば、双方が同一のローカルエリアネットワークに接続されていると仮定することができる。図 35 にその方法を示す。

【0014】

図 35 に示すように、あらかじめソース機器にシンク機器のネットワークアドレス A を登録しておく (ステップ S21)。コンテンツを送受信する際に、ソース機器は自ネットワークアドレスとシンク機器のネットワークアドレスを比較し (ステップ S22, S23)、一致すれば同一のローカルエリアネットワークに存在するものとして (ステップ S24)、コンテンツの送信を行う。その際、宛先がシンク機器のパケットの TTL フィールドを 1 にセットするように設定してもよい (ステップ S25)。一致しなければ、コンテンツの送受信処理を中止する (ステップ S26)。なお、この例ではソース機器が比較処理を行なっているが、逆にシンク機器が比較処理を行なってもよい。

【0015】

【特許文献 1】

特願 2002-19135 号

【特許文献 2】

特開 2001-285284 号公報

【0016】

【発明が解決しようとする課題】

しかしながら、ソース機器やシンク機器に所定の設定を行うことで、ソース機器とシンク機器が物理的に同一のローカルエリアネットワークに接続されていなくても、仮想的に同一サブネットに存在するように見せることで、前述したネットワークアドレスの比較による同一のローカルエリアネットワークの限定を回避することができる。

【0017】

VPNはその一例である。VPNとは、Virtual Private Networkの略で、インターネットに接続された遠隔地の計算機やルータ等の接続点とローカルエリアネットワークに接続された計算機が通信を行って仮想的にネットワークを構築することで、遠隔地の計算機がローカルネットワークに接続しているかのようにみせる技術の総称を指す。

【0018】

VPNの例としては例えば、L2TPやPPTP、IPSecなどがある。ここでは、L2TPを例にとって説明する。なお、L2TP、PPTP及びIPSecについてはIETFにより標準化が進んでおり、<http://www.ietf.org>にて取得可能に開示されている文書に説明が詳しい。

【0019】

図36はVPNを使ったネットワーク構成の一例を示す図である。図36に示すように、ソース機器B1とシンク機器C9、およびVPNサーバ機器D60が物理的なイーサネットセグメントA3に接続されており、同一のネットワークアドレスを持つことで、ローカルエリアネットワークZ61を構成している。またシンク機器A4とルータ機器E5は、同一のネットワークアドレスを持ち、ローカルエリアネットワークYを構成している。

【0020】

VPNサーバ機器D60はルーター機能を備え、インターネット6に接続されている。シンク機器A4にはグローバルなIPアドレスが割り振られており、VPNクライアント機能を使ってインターネット6を経由してVPNサーバ機器D60に接続して仮想ネットワークXを構築している。この仮想ネットワークにシンク機器A4が接続することになる。ここで重要なことは、シンク機器A4はVPNで接続

することにより、仮想的にソース機器B 1やシンク機器C 9と同一のネットワークアドレスが割り振られていることである。

【0021】

ここで、ソース機器B 1からシンク機器A 4へコンテンツを送信する際に、前述したネットワークアドレスの比較による配布範囲の限定方法を適用してみる。

【0022】

シンク機器A 4はソース機器B 1と同一のネットワークアドレスを持つため、ネットワークアドレスは一致してしまう。シンク機器A 4がインターネット6に接続していればたとえ世界の裏側に配置されていたとしても、ソース機器B 1はシンク機器A 4にコンテンツを送信することができてしまう。

【0023】

またソース機器B 1がIPパケットをTTL=1にセットしてシンク機器A 4に送信したとしてもTTLの値は容易に改変可能であるため、例えば、VPNサーバ機器D 60とソース機器Bの間にTTLの値を改変するような機器を設置されてしまった場合、パケットはシンク機器A 4に到達可能となってしまう。

【0024】

これは、ソース機器B 1とシンク機器A 4のサブネットアドレスが同一だとしても、必ずしもこれらの機器は物理的に同一のローカルエリアネットワーク（この場合、イーサネットセグメント）に存在するとは限らない場合があることを意味する。

【0025】

本発明は、このような点に鑑みてなされたものであり、その目的は、限られた受信装置だけにコンテンツを送信可能なコンテンツ送受信システム、コンテンツ送信装置、コンテンツ受信装置及びコンテンツ送受信方法を提供することにある。

【0026】

【課題を解決するための手段】

上述した課題を解決するために、本発明は、送信装置と、この送信装置からコンテンツを受信する少なくとも1台の受信装置と、を備えたコンテンツ送受信シ

システムにおいて、前記送信装置は、コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う第1の認証・鍵交換処理手段と、前記受信装置の機器識別情報を送信するよう前記受信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、前記受信装置のIP (Internet Protocol) アドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と前記機器識別情報登録手段に登録されている機器識別情報とが一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求を行った前記受信装置へのコンテンツの配布条件を変更する配布条件決定手段と、を有し、前記受信装置は、前記送信装置に対して前記コンテンツ送信要求を行うコンテンツ送信要求手段と、前記送信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報を前記送信装置に送信する機器識別情報送信手段と、を有する。

【0027】

また、本発明は、少なくとも1台の受信装置に対してコンテンツを送信するコンテンツ送信装置において、コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、前記受信装置の機器識別情報を送信するよう前記受信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、前記受信装置のIPアドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求を行った前記受信装置へのコンテンツの配布条件を変更する配布条件決定手段と、を備える。

【0028】

また、本発明は、送信装置からのコンテンツを受信するコンテンツ受信装置において、前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手

段と、コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を備える。

【0029】

また、送信装置と、この送信装置からコンテンツを受信する少なくとも1台の受信装置と、を備えたコンテンツ送受信システムにおいて、前記受信装置は、前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う第1の認証・鍵交換処理手段と、前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を有し、前記送信装置は、前記受信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報を前記受信装置に送信する機器識別情報送信手段と、コンテンツ送信要求を行った前記受信装置との間で、認証・鍵交換処理を行う第2の認証・鍵交換処理手段と、前記配布条件決定手段で決定された配布条件に従って、コンテンツの送信制御を行うコンテンツ送信制御手段と、を有する。

【0030】

また、本発明は、送信装置からのコンテンツを受信可能なコンテンツ受信装置において、前記送信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記送信装置からのコンテンツの受信を禁止するコンテンツ受信制御手段と、を備える。

【0031】

また、本発明は、少なくとも1台の受信装置に対してコンテンツを送信可能なコンテンツ送信装置において、前記受信装置に対して、該受信装置の機器識別情報検索を事前通知する事前通知手段と、前記受信装置のIPアドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、前記機器識別情報検索手段で検索された機器識別情報と、前記機器識別情報登録手段に登録された機器識別情報と、が一致するか否かを判定する比較判定手段と、前記受信装置から送信された、前記機器識別情報検索の事前通知に対する応答を受信したか否かを判定する要求応答受信判定手段と、前記比較判定手段及び前記要求応答受信判定手段による判定結果に基づいて、前記受信装置へのコンテンツの配布条件を決定する配布条件決定手段と、を備える。

【0032】

また、本発明は、送信装置と、この送信装置からコンテンツを受信する少なくとも1台の受信装置と、を備えたコンテンツ送受信システムにおいて、前記送信装置は、前記受信装置に対して、該受信装置の機器識別情報検索を事前通知する事前通知手段と、前記受信装置のIPアドレスに対応する前記機器識別情報を、前記受信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記受信装置から送信された前記機器識別情報を登録する機器識別情報登録手段と、前記機器識別情報検索手段で検索された機器識別情報と、前記機器識別情報登録手段に登録された機器識別情報と、が一致するか否かを判定する比較判定手段と、前記機器識別情報検索の事前通知に対する応答を受信したか否かを判定

する要求応答受信判定手段と、前記比較判定手段及び前記要求応答受信判定手段による判定結果に基づいて、前記受信装置へのコンテンツの配布条件を決定する配布条件決定手段と、を有し、前記受信装置は、前記送信装置からの前記機器識別情報要求を受信すると、自装置の前記機器識別情報及び機器識別情報の検索事前通知応答を前記送信装置に送信する自装置情報送信手段を有する。

【0033】

また、本発明は、少なくとも1台の受信装置に対してコンテンツを送信可能なコンテンツ送信装置において、前記受信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記受信装置へのコンテンツの送信を禁止するコンテンツ送信制御手段と、を備える。

【0034】

また、本発明は、送信装置からのコンテンツを受信するコンテンツ受信装置において、前記送信装置に対して、該送信装置の機器識別情報検索を事前通知する事前通知手段と、前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を備える。

【0035】

また、本発明は、送信装置と、この送信装置からコンテンツを受信する少なくとも1台の受信装置と、を備えたコンテンツ送受信システムにおいて、前記送信

装置は、前記受信装置から自装置の機器識別情報検索要求があったか否かを判定する機器識別情報検索判定手段と、前記機器識別情報検索判定手段により前記機器識別情報検索要求がなかったと判定された場合には、前記受信装置へのコンテンツの送信を禁止するコンテンツ送信制御手段と、を有し、前記受信装置は、前記送信装置に対して、該送信装置の機器識別情報検索を事前通知する事前通知手段と、前記送信装置に対してコンテンツ送信要求を行うコンテンツ送信要求手段と、コンテンツ送信要求先である前記送信装置との間で、認証・鍵交換処理を行う認証・鍵交換処理手段と、前記送信装置の機器識別情報を送信するよう前記送信装置に対して機器識別情報要求を送信する機器識別情報送信要求手段と、前記送信装置から送信された前記送信装置の機器識別情報を登録する機器識別情報登録手段と、前記送信装置のIPアドレスに対応する前記機器識別情報を、前記送信装置が接続されているネットワークから検索する機器識別情報検索手段と、前記検索された機器識別情報と、前記機器識別情報登録手段に登録されている機器識別情報と、が一致するか否かを判定する比較判定手段と、前記比較判定手段による一致判定結果に応じて、コンテンツ送信要求先である前記送信装置からのコンテンツ配布条件を決定する配布条件決定手段と、を有する。

【0036】

【発明の実施の形態】

以下、本発明に係るコンテンツ送受信システムについて、図面を参照しながら具体的に説明する。以下では、物理的なネットワークの一例としてイーサネットを用い、上位プロトコルにIPを使うものとする。もちろん、その他のプロトコル、例えばローカルエリアネットワークがIEEE1394で構成されていて、上位レイヤーとしてIPをエミュレーションしたIP over 1394であってもよい。

【0037】

図1は本発明に係るコンテンツ送受信システムの第1の実施形態の概略構成を示すブロック図である。図1のコンテンツ送受信システムは、イーサネットセグメントA10に接続されるシンク機器B11、シンク機器C12、ソース機器D及びルータ機器F13と、ルータ機器F13にインターネット14を介して接続されるソース機器A15とを有する。シンク機器B11はVPNサーバ機能を持

ち、ソース機器A15はVPNクライアント機能を持つものとする。

【0038】

シンク機器B11, C12はそれぞれ同一のイーサネットセグメントA10に接続されており、同一のネットワークアドレスを持つことにより、ローカルエリアネットワークを構成している。

【0039】

ここで、コンテンツの配布範囲を一定の範囲内（ここではイーサネットセグメントA10）に限定する方法について説明する。すなわち、物理的なイーサネットセグメントA10に接続されたシンク機器B11, C12には、ソース機器D（要注意：図面1を修正）からのコンテンツの送受信を許可するが、VPN機能を用いて別のイーサネットセグメントに接続されたソース機器A15からはコンテンツを送受信しないようにする。

【0040】

本実施形態では、仮にシンク機器とソース機器がVPNによって仮想的なネットワークを構築し、同一のローカルエリアネットワークに接続しているかのような構成をとっていたとしても、物理的にイーサネットセグメントに接続されている場合と、仮想的に接続している場合とを区別する点に特徴がある。

【0041】

なお、ここではコンテンツの送受信にあたり、機器の認証・鍵交換及びコンテンツ暗号化・復号化の仕組みとしてDTCPを一例として説明する。DTCPとはDigital Transmission Contents Protectionの略で、IEEE1394やUSBなどでデファクトスタンダードとなっている著作権保護方式である。著作権保護が必要なAVデータなどのコンテンツに対して、送信機器と受信機器との間で認証・鍵交換を行い、AVデータを暗号化して転送する仕組みが備わっている（例えば<http://www.dtcpa.com>にて取得可能に開示されている文書に説明が詳しい）。

【0042】

図2はソース機器A15とソース機器D16の内部構成の一例を示すブロック図である。図2に示すように、ソース機器A15及びD16は、イーサネットの物理レイヤ処理を実行するネットワークインターフェース部21と、データリン

クレイア処理を実行する通信処理部 22 と、シンク機器のネットワークインターフェースの MAC アドレス（以下、単に MAC アドレスと示す）を MAC アドレステーブル 23 に記録する MAC アドレス記録部 24 と、シンク機器の IP アドレスから MAC アドレスを検索するシンク機器 MAC アドレス検索処理部 25 と、シンク機器 MAC アドレス検索処理部 25 から取得した MAC アドレスと MAC アドレス記録部 24 に記録されたものとが一致しているか否かの検査を行う MAC アドレス比較処理部 26 と、著作権保護のために DTCP 認証・鍵交換処理を行う認証・鍵交換処理部 27 と、送受信するデータを暗号・復号化する DTCP 暗号処理部 28 と、シンク機器に送信するコンテンツデータや DTCP 管理データを IP パケットに変換するパケット処理部 29 と、VPN サーバとして VPN クライアントから VPN 接続要求を受け付け、VPN 接続を行う VPN サーバ部 40 と、コンテンツをパケット処理部 29 に供給するコンテンツ供給部 30 とを有する。ここでは VPN のプロトコルの一例として L2TP を用いるものとする。L2TP とは、レイヤ 2 トンネリングプロトコル（Layer2 Tunneling Protocol）の略であり、VPN の実現手段として広く利用されている。L2TP については、IETF により標準化が進んでおり、<http://www.ietf.org> にて取得可能に開示されている文書に説明が詳しい。

【0043】

また、ここではソース機器 A 15 とソース機器 D 16 を同一の構成として示してきたが、ソース機器 D 16 は必ずしも VPN サーバ部 40 を備えている必要はない。なぜならば、ソース機器 D 16 とシンク機器 B 11 及びシンク機器 C 12 は同一のイーサネットセグメント上に接続されており、VPN を介して接続することが不要なためである。

【0044】

なお、比較処理とは、コンテンツ送信先であるシンク機器の IP アドレスやデバイス ID に対応する MAC アドレスが MAC アドレステーブル 23 に記録されており、かつ値が一致されているか否かの検索処理を行うことを示す。

【0045】

図 3 は MAC アドレステーブル 23 の構造を示す図である。図 3 に示すように、各シンク機器に対応した IP アドレス、MAC アドレス及び DTCP デバイス ID がレコ

ード毎に記録される。MACアドレス比較処理部26は、MACアドレステーブル23を使って、シンク機器から取得したIPアドレスやデバイスIDをキーとしてMACアドレスを検索する。

【0046】

図4はシンク機器B11、C12の内部構成の一例を示すブロック図である。図4に示すように、シンク機器B11、C12はイーサネット物理レイヤ処理を実行するネットワークインターフェース部31と、データリンクレイヤ処理を実行する通信処理部32と、ネットワークインターフェース部31に記憶されているMACアドレスを取得してソース機器に送信するMACアドレス送信部33と、VPNクライアントとしてインターネットを経由してVPNサーバに接続するVPNクライアント部34と、著作権保護のためのDTCP認証・鍵交換処理を行うDTCP認証・鍵交換処理部35と、送受信するデータを暗号・復号化するDTCP暗号処理部36と、ソース機器から受信したIPパケットをコンテンツデータやDTCP管理データに変換するパケット処理部37と、復号化したコンテンツを表示装置などに出力したり蓄積するための処理を行うコンテンツ処理部38とを有する。

【0047】

ここではシンク機器B11とC12が同一の構成として示してきたが、ソース機器Dとシンク機器C12が通信を行なう場合には、VPNで接続する必要はないため、シンク機器がVPNクライアント部34を備えていない構成もありうる。

【0048】

なお、ここではソース機器A15がVPNサーバ部40を有し、シンク機器B11がVPNクライアント部34を有する構成を示したが、ソース機器A15とシンク機器B11がVPNにて通信を行うことが重要であり、VPNの機能を入れ替えた構成、すなわちソース機器A15がVPNクライアント部34を有し、シンク機器B11がVPNサーバ部40を有する構成となってもよい。

【0049】

図5及び図6は本実施形態の通信システムの処理手順を示す図、図7はソース機器A15の処理手順を示す図である。以下、まず最初に、図6及び図7に沿っ

てソース機器Dからシンク機器C 1 2にコンテンツを送信する例を説明する。

【0050】

まず、シンク機器C 1 2からソース機器D 1 6へコンテンツの送信要求がなされると（ステップS 1）、DTCP認証・鍵交換処理が行なわれる（ステップS 1 2）。

【0051】

なお、コンテンツの送信要求がなされた時点で、宛先のIPアドレスがシンク機器C 1 2に対して著作権保護に関する認証・鍵交換等の管理データ及びコンテンツを送信する際にはIPパケットのTTLフィールドを1に設定してもよい（ステップS 2, S 1 1）。また、従来の技術で述べたように、シンク機器とソース機器のネットワークアドレスが一致するか否かの比較処理を行なってもよい。この場合、シンク機器C 1 2とソース機器D 1 6のネットワークアドレスが異なる場合には、所定のエラー処理を行い、通信を中止すればよい。これらの処理は、DTCP認証・鍵交換処理を行う前に行ってもよいし、同処理の途中あるいは後に行ってもよい。

【0052】

DTCP認証・鍵交換処理が成功すると（ステップS 3）、ソース機器D 1 6はシンク機器C 1 2に対してMACアドレスの送信を要求するコマンドを送信する（ステップS 4）。このコマンドは独立したコマンドでもよいし、DTCPで定義されるコマンド群に「MACアドレス要求コマンド」を追加したものでもよい。シンク機器C 1 2はMACアドレス要求コマンドを受信すると、アドレス送信部33を介してソース機器D 1 6にMACアドレスを送信する（ステップS 5）。

【0053】

この時、通信経路上でMACアドレスが改ざんされていないことを示すために署名をつけてもよい。この署名の方法は、例えばISO/IEC14888のような、よく知られた方法を用いればよい。

【0054】

ソース機器D 1 6はシンク機器C 1 2のMACアドレスを取得すると（ステップS 1 3）、MACアドレステーブル23に登録する（ステップS 6, S 1 4）。こ

のとき、MACアドレスとシンク機器C 1 2のIPアドレスやDTCPデバイスIDを組として記録してもよい。

【0055】

以上は、MACアドレスをシンク機器C 1 2からネットワークを経由して受信することで、シンク機器C 1 2のMACアドレステーブル23に登録する方法である。登録方法については、この他にも種々の方法が考えられる。例えば、(1)あらかじめ利用者がソース機器D 1 6にシンク機器C 1 2のMACアドレスをボタン等のインターフェースを用いて入力する方法、(2)シンク機器C 1 2のMACアドレスが記録されたカード等を用いてソース機器DのMACアドレステーブルに登録する方法などが考えられる。

【0056】

次に、ソース機器D 1 6はIPアドレスからMACアドレスの問い合わせを行うパケットをイーサネットセグメントA 1 0に送信する。この仕組みはよく知られた方法、例えばRFC826にて規定されたARP (アドレス解決プロトコル)を用いればよい。物理的に同一セグメントに接続されていれば、応答としてIPアドレスを持つホストは自機器に付与されたMACアドレスを返す(ステップS 8, S 1 5)。例えば、ソース機器D 1 6がIPアドレス192.168.1.5に対してARPのリクエストを送信したとすると、IPアドレスが192.168.1.5に設定されたシンク機器C 1 2はその応答として、ソース機器D 1 6に自身のMACアドレス「CC:CC:CC」を返すことになる。

【0057】

次に、ソース機器D 1 6は、MACアドレス要求コマンドの結果として取得したシンク機器C 1 2のMACアドレスとARPによって取得したMACアドレスが一致するかの比較処理を行う(ステップS 9, S 1 6)。もし二つの値が一致していれば処理を継続する(ステップS 1 7, S 1 8)。

【0058】

上述したステップS 7にて、MACアドレステーブル23から通信相手のシンク機器のMACアドレスを検索する際に、検索のキーとしてIPアドレスだけでなく、デバイスIDをキーとしてMACアドレスを検索してもよい。

【0059】

上述したステップS16の比較処理において、MACアドレスが一致していなければ所定のエラー処理を行い、通信を中止する（ステップS10，S19）。また、ARPによってシンク機器C12のMACアドレスが取得できない場合も所定のエラー処理を行い、通信を中止する。この例では、事前にMACアドレスリストに登録した値とARPによって取得した値は同一であるため、コンテンツ送信処理が行なわれる。

【0060】

次に、ソース機器A15からシンク機器B11にコンテンツを送信する例を図5に示す。ソース機器A15はVPNにてシンク機器B11に接続されており、通信可能な状態にある。ソース機器A15がシンク機器B11にMACアドレスを要求し、IPよりも上位のプロトコルでシンク機器B11のMACアドレスを取得し、記録する処理（ステップS6）まではソース機器Dからシンク機器C12と同様の方法で行なえばよい。ソース機器A15はシンク機器B11のIPアドレスからMACアドレスの問い合わせを行うパケット（例えばARPパケット）を、ソース機器A15が接続されている不図示のイーサネットセグメントに送信する。この場合、シンク機器B11は不図示のイーサネットセグメントに接続されていないため、シンク機器B11が応答として自身のMACアドレス「CC:CC:CC」を返すことはない。このため、ソース機器A15がシンク機器B11のMACアドレスを取得することはない。このため、MACアドレス比較処理は失敗する。これにより、ソース機器はエラー処理を行い、シンク機器B11に対してコンテンツを送信することなく通信を終了する。

【0061】

なお、MACアドレス不一致の際のエラー処理や、シンク機器とのコネクション切断時に、シンク機器に関するレコードを記憶しておいてもよいし、消去してもよい。例えばシンク機器のIPアドレスがDHCPによって割り振られた場合、次回接続時にIPアドレスは変化する可能性があるため、消去した方が、テーブルに割り当てる記憶容量を節約でき、機器の構成を簡単にすることができる。

【0062】

さて、これまでDTCP認証・鍵交換処理によって、認証された場合にのみMACアドレスの確認処理を行う例を示した。この他にもMACアドレスの確認を行うには、（１）シンク機器がコンテンツ要求をソース機器に送信する際にDTCPのコンテンツ要求コマンドとルーター共にMACアドレスを付加して送信する方法、（２）DTCP認証・鍵交換処理に先立ち、MACアドレスの確認処理を行う方法などがある。

【0063】

ここで重要なことは、シンク機器がソース機器にイーサネットよりも上位のプロトコルでMACアドレスを送信する機能を持ち、イーサネット上でIPアドレスからMACアドレスを検索する処理で得たMACアドレスとを比較することで、ソース機器とシンク機器が同一サブネットであっても、イーサネットセグメントに物理的に接続されているのか、そうでないかを判別することができる点である。

【0064】

仮に、ソース機器A15のMACアドレス要求に対する応答として、ソース機器A15と物理的に同一のイーサネットセグメントに接続されている不図示のルーター機器が、MACアドレスを偽り、シンク機器B11のMACアドレスと同一のMACアドレスを送信したとしても、ソース機器A15はその偽ったMACアドレスにイーサネットパケットを送信するため、シンク機器B11がこのパケットを受信することができず、コンテンツの配布範囲を限定する目的は達成できる。

【0065】

次に、図8に示すように、ソース機器とシンク機器との間にVPNサーバ機器53が接続されている場合のコンテンツ送受信について説明する。図8のコンテンツ送受信システムは、同一のイーサネットセグメントA50に接続されるソース機器B51、シンク機器C52、VPNサーバ機器F53及びルータ機器D54と、インターネット55を介してVPNサーバ機器F53に接続されるシンク機器A56と、イーサネットセグメントB57に接続されるシンク機器E58とを備えている。

【0066】

ソース機器B51、シンク機器C52、VPNサーバ機器F53及びルータ機器D54はそれぞれ同一のネットワークアドレスを持つことにより、ローカルネッ

トワークを構成している。

【0067】

シンク機器A56には、グローバルなIPアドレスが割り振られており、VPNクライアント機能を使ってインターネットを経由してVPNサーバ機器Dに接続可能な状態にある。

【0068】

図8のコンテンツ送受信システムにおいて、ソース機器B51からVPNサーバ機器F53を経由して、仮想的に接続しているシンク機器A56にコンテンツを送信する場合を考える。

【0069】

まず、ソース機器B51がシンク機器A56からMACアドレスを受信し、登録するまでは上記手続きと同じでよい。その後、ソース機器B51はシンク機器A56のIPアドレスからMACアドレスの問い合わせを行うパケットをイーサネットセグメントA50に送信する。

【0070】

シンク機器A56は物理的なイーサネットセグメントA50に接続されていないため、VPNサーバ機器F53が自身のMACアドレスを代理でシンク機器A56のMACアドレスとして応答を返す。ソース機器B51はこれら二つのMACアドレスの比較処理を行うが、シンク機器E58とVPNサーバ機器F53のMACアドレスは異なるため、値は一致しない。このため、コンテンツ送信処理は中止される。

【0071】

次に、ソース機器B43からシンク機器E47にコンテンツを送信する場合を考える。ソース機器B43はシンク機器E47にMACアドレスを要求し、IPよりも上位のプロトコルでシンク機器E47のMACアドレスを取得する。しかしこの構成では、ソース機器B43の接続するイーサネットセグメントA50と、シンク機器Eの接続するイーサネットセグメントB57は異なる。従って、ソース機器B43は、シンク機器E47のIPアドレスからMACアドレスの問い合わせ処理を行なうパケットを送信したとしても、当該パケットはルータ機器によってシンク機器Eに転送されることはなく、ソース機器B43はシンク機器E

47からMACアドレスを受信することはない。これにより、ソース機器B51で行なうMACアドレスの比較処理は失敗し、コンテンツの送信処理が中止される。

【0072】

以上の処理により、図8のソース機器B51は、同一イーサネットセグメントA50に接続されるシンク機器C52にはコンテンツの送受信を許可するが、VPNサーバ機器F53を介して接続されるシンク機器A56や、ルータ機器D54を介して異なるイーサネットセグメントB57に所属するシンク機器E58に対するコンテンツの送受信を確実に禁止できる。

【0073】

このように、本実施形態によれば、例えば図8のような構成のコンテンツ送受信システムにおいて、ソース機器B51は同一イーサネットセグメントA50に接続されているシンク機器C52のみにコンテンツの送受信を許可するため、例えばVPNサーバ機器F53を介して接続されるシンク機器等へのコンテンツの送受信を確実に禁止できる。これにより、コンテンツの不正な送受信を防止できる。

【0074】

以上は、シンク機器A56にVPNクライアントが備わっており、VPNサーバF53を経由してイーサネットセグメントAに接続する構成について説明をしてきたが、本実施形態は、ソース機器にVPNクライアントが備わっている構成になっていてもよい。

【0075】

図9はソース機器とシンク機器の接続関係を第1の実施形態とは逆にした場合の概略構成を示すブロック図である。図9のコンテンツ送受信システムは、図8と異なり、VPNクライアント機能を持ち、インターネット15を経由してVPNサーバ機器F13に接続されるソース機器A41と、イーサネットセグメントA42に接続されるシンク機器B43、シンク機器C44及びルータ機器D45と、ルータ機器D45にイーサネットセグメントB46を介して接続されるシンク機器E47とを有する。

【0076】

すなわち、VPNサーバ機器F 13に接続されるシンク機器B 43及びシンク機器C 44は、VPNサーバF 13を経由してソース機器A 41と通信可能な位置に存在する。しかし、ソース機器A 41とシンク機器B 43、C 44は異なるローカルエリアネットワークに接続されているため、著作権を保護すべきコンテンツの送受信は許可されるべきではないものとする。

【0077】

ここで、ソース機器A 41がシンク機器B 43に対してMACアドレスを要求し、IPよりも上位のプロトコルでシンク機器B 43のMACアドレスを取得する。ソース機器A 41はシンク機器B 43のIPアドレスからMACアドレスの問い合わせを行うパケット（例えばARPパケット）を、ソース機器A 41が接続されている不図示のイーサネットセグメントに送信する。この場合、シンク機器B 43は不図示のイーサネットセグメントに接続されていないため、シンク機器B 43が応答として自身のMACアドレス「BB:BB:BB」を返すことはない。このため、ソース機器A 41がシンク機器B 43のMACアドレスを取得することはなく、MACアドレス比較処理は失敗する。これにより、ソース機器はエラー処理を行い、シンク機器B 43に対してコンテンツを送信することなく通信を終了する。これにより、VPNを介したコンテンツの送受信を防ぐことができ、ソース機器A 41がコンテンツの配布範囲をソース機器A 41のローカルエリアネットワーク内に制限することができる。

【0078】

（第2の実施形態）

第2の実施形態はシンク機器とソース機器の間にVPNサーバ機器とVPNクライアント機器を設置し、VPN機器が二つのネットワークをトンネリングする構成にしたものである。

【0079】

図10はシンク機器A 48とソース機器B 43の間にVPNサーバ機器F 13とVPNクライアント機器G 49を設置し、VPNサーバ機器F 13とVPNクライアント機器G 49が二つのネットワークをトンネリングするコンテンツ送受信システムの

ブロック構成を示している。図10で示したコンテンツ送受信システムの形態におけるソース機器の内部構成は図11のようなブロック図で表され、シンク機器の内部構成は図12のようなブロック図で表される。

【0080】

図1や図8と異なり、図10のコンテンツ送受信システムは、シンク機器A48とソース機器B43との間にVPNサーバ機器F13とVPNクライアント機器G49があり、それぞれのネットワークを接続している。しかしながら、ソース機器B43の所属するイーサネットセグメントA42とシンク機器A48の所属するイーサネットセグメントB46は互いに異なるため、ソース機器B43のMACアドレス検索要求からシンク機器A48のMACアドレスを取得することはできず、比較処理は失敗する。これにより、シンク機器A48がソース機器B43の所属するイーサネットセグメントA42に存在しないことを確認できる。

【0081】

このように、第2の実施形態においても、MACアドレスを比較して、比較結果が一致した場合のみコンテンツの送信を許可することにより、異なるイーサネットセグメントに接続されたシンク機器へのコンテンツ送信を確実に禁止できる。

【0082】

上述した各実施形態において、ソース機器からの要求に従ってシンク機器が自己のMACアドレスを送信する際、MACアドレスとともに電子署名を添付して送信してもよい。ソース機器は、シンク機器からのMACアドレスに電子署名が添付されていた場合は、MACアドレスが改ざんされているか否かの検証処理を行い、改ざんされていない場合にのみMACアドレスをMACアドレステーブルに記録する。これにより、MACアドレスの偽造を確実に防止でき、セキュリティ性能の向上が図れる。

【0083】

上述した各実施形態では、ソース機器の内部でMACアドレスの比較を行う例を説明したが、コンテンツの受け取り側であるシンク機器の内部でMACアドレスの比較を行ってもよい。例えば、図1に示した構成でのソース機器A15に対応するシンク機器とソース機器の役割を入れ替えた構成にした場合のソース機器の内

部構成は図13のようなブロック図で表され、シンク機器B11の内部構成は図14のようなブロック図で表される。

【0084】

この場合、ソース機器が自機器のMACアドレスをシンク機器に送信し、シンク機器内でのMACアドレスの比較結果が一致した場合のみ、ソース機器からコンテンツの受信を受付を行ったり、場合によっては受信拒否のメッセージをシンク機器に対して送信したりすることで、コンテンツの送信先を限定することができる。

【0085】

図15はVPN機器の接続形態の種類を示す図である。VPN機器は、それ自身でルーティングを行うため、TTLの減算を行う。すなわち、図15に示すようにVPN機器を介してシンク機器とソース機器が通信を行うには、IPヘッダのTTLフィールドを適切な値以上に設定しなければならない。

【0086】

例えば、図15の環境Aの構成では、VPN機器がルーティングを行うため、各VPN機器でTTLフィールドの減算を行う。したがって、シンク機器A-Aとソース機器A-Bが通信を行うには、TTLの値を3以上に設定しなければならない。同様に、環境Bの構成でも、シンク機器B-Aとソース機器B-Bが通信を行うには、TTLの値を3以上に設定しなければならない。

【0087】

従って、TTLの値を1に設定すれば、環境Aや環境BではVPN装置を介したコンテンツの配布を制限することができる。ここで注意すべきは、TTLフィールドが容易に改変可能だということである。例えば悪意ある利用者がTTLフィールドを一定の値に増加させるTTL改変装置をソース機器とVPN機器の間に設置したとすると、ソース機器、及びシンク機器が想定する配布範囲を超えてコンテンツを送受信することが可能となってしまう。

【0088】

しかしながら、上述した手法を用いれば、例えTTL改変装置を設置されたとしても、ソース機器とシンク機器は物理的な同一セグメントに所属していないため

、依然としてARPによって互いのMACアドレスを知ることができず、TTL改変装置の影響を受けることはない。

【0089】

すなわち、本実施形態によれば、環境A、B、Cに係らず統一的にVPNの存在を検出することができ、コンテンツの配布範囲を限定することができる。

【0090】

(第3の実施形態)

上述した第1及び第2の実施形態において、ソース機器と物理的に同一のイーサネットセグメントに接続されたルータ機器やVPN機器にシンク機器と同一のMACアドレスを設定してしまうと、ソース機器とシンク機器が物理的に同一のイーサネットセグメントに接続されているか否かを正確に判断できなくなるおそれがある。

【0091】

そこで、以下に説明する第3の実施形態は、このような不具合を解決することを特徴とする。

【0092】

図16は本発明に係るコンテンツ送受信システムの第3の実施形態の概略構成を示すブロック図である。図16のVPNサーバ機器F53は、図8と異なり、シンク機器Aと同一のMACアドレスの値AA:AA:AAを持つ。

【0093】

原則として、MACアドレスは、各製造ベンダにより、物理的なネットワークインターフェースごとに異なる値が付与されることになっている。しかし、この原則から外れてMACアドレスが一致してしまった場合や、悪意のある利用者がMACアドレス比較のチェック処理を回避するために、VPNサーバ、もしくはルーター機器にシンク機器と同じ値のMACアドレスをつけたとする。

【0094】

この場合、ソース機器B51がイーサネット上でIPアドレスからMACアドレスを検索する処理(例えばARP)で得るMACアドレスの値はVPNサーバ機器のMACアドレスであるAA:AA:AAとなる。その結果、上位のプロトコルによって取得したシンク

機器AのMACアドレスAA:AA:AAと、IPアドレスからMACアドレスを検索する処理で得るMACアドレスの値は一致してしまうため、ソース機器とシンク機器が同一のイーサネットセグメントに物理的に接続されているのか、そうでないのかを判別することができない。

【0095】

第3の実施形態では、仮にソース機器に物理的に同一のイーサネットセグメントに接続されたVPN機器またはルーター機器が、シンク機器と同一のMACアドレスを保持していたとしても、ソース機器とシンク機器間でアドレス解決要求を確実に行ったかどうかを確認することで、ソース機器とシンク機器が物理的に同一のセグメントにいるのか、そうでないのかを確認できるようにしている。

【0096】

図17は第3の実施形態におけるソース機器B51の内部構成を示すブロック図である。図2との相違点は、シンク機器にIPアドレスからMACアドレスを検索するためのメッセージを送信する前に、「これからMACアドレス検索要求を送る」ことを明示的に通知するメッセージ（以下、このメッセージをMACアドレス検索事前通知と呼ぶ）を送信したり、検索事前通知応答がシンク機器から送信されたかどうか確認する処理を行うMACアドレス検索事前通知処理部62を有する点である。

【0097】

図18は第3の実施形態におけるシンク機器A56の内部構成を示すブロック図である。図4と異なる点は、ソース機器から送信されたMACアドレス検索事前通知を受信して所定の処理を行うMACアドレス検索事前通知受信処理部63を有する点である。

【0098】

図19は第3の実施形態の処理手順を示すシーケンス図であり、ソース機器とシンク機器が物理的に同一のセグメントに存在する場合（例えば、図8に示すソース機器B51とシンクC52が通信を行う場合）の処理手順を示している。

【0099】

ここでは、説明を簡略化するために、図5に示すようなDTCP認証・鍵交換処理

(ステップS 3)、MACアドレス要求(ステップS 4)及びMACアドレス送信(ステップS 5)が行われており、DTCP認証・鍵交換が成功し、ソース機器がシンク機器のMACアドレスを取得しているものとする。

【0100】

まず、ソース機器はIPアドレスからMACアドレスを検索する要求メッセージとMACアドレス検索事前通知とをシンク機器に送信する(ステップS 31～S 33)。MACアドレス検索事前通知はイーサネットよりも上位のプロトコル(例えばIPパケット)にて送信すればよい。なお、これらのメッセージは同時に送信してもよいし、別々に送信してもよい。

【0101】

シンク機器は、MACアドレス検索の応答として、自機器のMACアドレスをソース機器に送信する(ステップS 34)。また、シンク機器は、ソース機器から送信されたMACアドレス検索を受信したことを記録しておく。

【0102】

ソース機器はMACアドレス検索要求によって受信したMACアドレスと事前に取得したMACアドレスとの比較処理を行う(ステップS 35)。ここではMACアドレスが一致するため、比較処理は成功し、ソース機器はコンテンツをシンク機器に送信する(ステップS 36)。

【0103】

一方、シンク機器はMACアドレス検索要求を受信しているか否かの確認処理を行う(ステップS 37)。ここでは、もしもソース機器からMACアドレスを検索する要求メッセージを受信していれば、処理を継続する(ステップS 38)。MACアドレス検索要求を受信していなければ、処理を中止するものとする。この場合、シンク機器はステップS 33でMACアドレス検索要求を受信しているため、このチェック処理は成功し、コンテンツの受信が開始される。

【0104】

図20はソース機器とシンク機器が物理的に同一のセグメントに存在しない場合(例えば図8に示すソース機器B51とシンク機器A56が通信する場合)における第3の実施形態の処理手順を示すシーケンス図である。

【0105】

図19の場合と同様に、まず、ソース機器はIPアドレスからMACアドレスを検索する要求メッセージとMACアドレス検索事前通知とをシンク機器に送信する（ステップS41，S42）。

【0106】

MACアドレス検索事前通知は、イーサネットよりも上位のプロトコルでシンク機器に送信されるため、途中でVPNサーバが存在しても、シンク機器はMACアドレス検索事前通知を受信する。

【0107】

ところが、IPアドレスからのMACアドレス検索要求に関しては、シンク機器は物理的に同一のイーサネットセグメントに接続しておらず、VPNサーバ機器が代理で応答してしまうため（ステップS43）、シンク機器はこの検索要求を受信できない。

【0108】

ここで、仮にVPNサーバ機器のMACアドレスとシンク機器のMACアドレスが一致していた場合、ソース機器でのMACアドレス比較処理は成功してしまうため（ステップS44）、ソース機器はシンク機器が物理的に同一のイーサネットセグメントに存在しないにも関わらず、コンテンツを送信してしまう（ステップS45）。

【0109】

一方、シンク機器は、MACアドレスの検索要求メッセージを受信しているか否かを確認し（ステップS46）、この要求メッセージを受信していないことがわかると、コンテンツの受信を中止する（ステップS47）。そして、ソース機器に対してコンテンツの送信中止依頼メッセージを送信し（ステップS48）、ソース機器は当該メッセージを受信するとシンク機器に対してコンテンツの送信を中止するようにしてもよい（ステップS49）。

【0110】

このように、第3の実施形態では、シンク機器がMACアドレスを検索する要求メッセージを受信したか否かによって、仮にソース機器とシンク機器の間に、I

PアドレスからMACアドレスを検索する要求に対してMACアドレスを偽って応答する機器が存在していたとしても、ソース機器とシンク機器が物理的に同一のセグメントにいるのか、そうでないのかを確認することができる。

【0111】

なお、第3の実施形態では、シンク機器がソース機器からMACアドレス検索を受信できれば、ソース機器からMACアドレス検索事前通知をシンク機器に送信する必要は必ずしもない。ただし、MACアドレスを検索する要求メッセージがソース機器から送られたものであることを確認するためには、MACアドレス検索事前通知にソース機器のMACアドレスやIPアドレス、もしくはその両方を含めてシンク機器に送信すればよい。これにより、MACアドレスの検索要求をシンク機器が受信した際に、それがソース機器からなされたものであるか、そうでないかを区別することが出来る。

【0112】

また、シンク機器は、MACアドレス検索事前通知を受信することにより、MACアドレス検索を監視する必要性を把握できるため、MACアドレス検索事前通知を受信するまではMACアドレス検索を監視する必要性がなくなり、平常時におけるシンク機器の処理負荷を軽減することができる。

【0113】

(第4の実施形態)

第4の実施形態は、シンク機器がソース機器と同一のセグメントに存在する可否かを第3の実施形態とは異なる処理手順で確認するものである。

【0114】

図21はソース機器の第4の実施形態の内部構成を示すブロック図である。図21のソース機器は、図17のソース機器の構成に加えて、シンク機器からのMACアドレス検索事前通知応答が受信されたか否かを判断するMACアドレス検索事前通知応答受信処理部64を有する。

【0115】

図22はシンク機器の第4の実施形態の内部構成を示すブロック図である。図22のシンク機器は、図18のシンク機器の構成に加えて、ソース機器からのMA

Cアドレス検索事前通知に対する応答であるMACアドレス検索事前通知応答をソース機器に送信する制御を行うMACアドレス検索事前通知応答処理部65を有する。

【0116】

図23は第4の実施形態の処理手順を示すシーケンス図であり、ソース機器とシンク機器が物理的に同一のセグメントに存在する場合（例えば、図8に示すソース機器B51とシンクC52が通信を行う場合）の処理手順を示している。なお、ここでも説明を簡単にするために、図19、図20と同様に、DTCP認証・鍵交換は成功し、ソース機器が上位のプロトコルでシンク機器のMACアドレスを取得しているものとする。

【0117】

まず、ソース機器はIPアドレスからMACアドレスを検索する要求メッセージとMACアドレス検索事前通知とをシンク機器に送信する（ステップS51、S52）。なお、これらのメッセージは同時に送信してもよいし、別々に送信してもよい。

【0118】

シンク機器は、MACアドレス検索要求の応答として、自機器のMACアドレスと検索事前通知応答とを含むメッセージをソース機器に送信する（ステップS53）。この検索事前通知応答はイーサネットよりも上位のプロトコル（例えばIPパケット）にて送信すればよい。また、検索事前通知応答のメッセージに、検索要求元、または検索結果送信先のMACアドレスを含めて送信してもよい。

【0119】

ソース機器は、IPアドレスからのMACアドレス検索の応答として、MACアドレスと検索事前通知応答のメッセージを受信する（ステップS54）。なお、このメッセージメッセージが改変されていないことを示すために、シンク機器が署名をつけたり、タイムスタンプをつけて送信し、ソース機器でこの署名を確認する処理を付け加えてもよい。

【0120】

ソース機器はMACアドレス検索要求によって受信したMACアドレスとMACアドレ

ス要求によって事前を取得したMACアドレスとの比較処理を行う（ステップS 55）。ここではMACアドレスが一致するため、比較処理は成功する。

【0121】

また、ソース機器は、検索事前通知応答を受信しているか否かの確認を行う（ステップS 56）。この確認処理は、もしもシンク機器から検索事前通知応答メッセージを受信していれば処理を継続し、受信していなければ処理を中止するものとする。ここでは、ステップS 54でMACアドレス検索事前通知応答を受信しているため、このチェック処理は成功し、コンテンツの送信が開始される（ステップS 57）。

【0122】

なお、検索事前通知応答メッセージにタイムスタンプが含まれている場合、タイムスタンプT1の値がソース機器がMACアドレス検索事前通知を送った時刻T0よりも後で、なおかつMACアドレスを受信した時刻T2よりも前であることを確認してもよい。

【0123】

図24はソース機器とシンク機器が物理的に同一のセグメントに存在しない場合（例えば、図8に示すソース機器B 51とシンク機器A 56が通信する場合）における第4の実施形態の処理手順を示すシーケンス図である。

【0124】

まず、ソース機器はIPアドレスからのMACアドレス検索とMACアドレス検索事前通知とをシンク機器に送信する（ステップS 61, S 62）。MACアドレス検索事前通知はイーサネットよりも上位のプロトコルで送信されるため、シンク機器によって受信される。ところが、IPアドレスからのMACアドレス検索要求に関しては、シンク機器は物理的に同一のイーサネットセグメントに接続しておらず、VPNサーバ機器が代理で応答してしまうため（ステップS 63）、シンク機器は受信できない。このため、シンク機器はIPアドレスからのMACアドレス検索の応答とMACアドレス検索事前通知応答とをソース機器に送信することはない。

【0125】

一方、ソース機器は、VPNサーバ機器からMACアドレスを受信する。ここで、仮

にVPNサーバ機器のMACアドレスとシンク機器のMACアドレスが一致していた場合、ソース機器でMACアドレス比較処理は成功してしまう（ステップS64）。しかし、検索事前通知応答は受信していないため、この確認処理は失敗し（ステップS65）、ソース機器はコンテンツの送信を中止する（ステップS66）。

【0126】

ここで注意すべきは、IPアドレスからMACアドレスを検索する要求メッセージはソース機器に限らず、一般のルーター機器などが送信することである。このため、シンク機器はどの要求メッセージに応答するMACアドレス検索事前通知応答をソース機器に送ればよいのかわからない。そのため、MACアドレス検索事前通知にて、ソース機器のIPアドレス、MACアドレスまたはその両方を送信することで、シンク機器は特定のIPアドレスもしくはMACアドレスから送信される要求メッセージに対してMACアドレス検索事前通知応答を送ればよいのか区別することができる。

【0127】

このように、第4の実施形態では、ソース機器からシンク機器に上位レイヤによりMACアドレス検索事前通知を送信するため、たとえソース機器とシンク機器の間に、シンク機器と同じMACアドレスを持つルータ機器やVPN機器が存在していたとしても、この通知に対する応答があったか否かで、シンク機器がソース機器と同一のセグメントに接続されているか否かを正確に判断でき、コンテンツの著作権保護が図れる。

【0128】

また、このMACアドレス検索事前通知とその応答は、コンテンツの著作権保護を目的したものであり、この判断を誤らせるために、MACアドレス検索事前通知に対する応答を偽って送信するような機器を設置することは、コンテンツの著作権保護を迂回するために意図的に設置したとみなすことができる。

【0129】

なお、以上では、MACアドレス検索事前通知とMACアドレス検索事前通知応答は、イーサネットよりも上位のレイヤーを用いることを前提としてきたが、DTCPで定義されるコマンド群の一つとして定義してもよい。この場合、DTCP認証・鍵交

換の処理の一部として、MACアドレス検索事前通知、及びMACアドレス検索事前通知応答を実現することができるため、機器の構成を簡略化することができる。

【0130】

(第5の実施形態)

上述した第5の実施形態では、ソース機器がMACアドレス検索事前通知をシンク機器に送信し、シンク機器がMACアドレス検索事前通知応答をソース機器に送信する構成について説明したが、以下に説明する第5の実施形態は、シンク機器がMACアドレス検索事前通知をソース機器に送信し、ソース機器がMACアドレス検索事前通知応答をシンク機器に送信するものである。

【0131】

図25はソース機器の第5の実施形態の内部構成を示すブロック図である。図25のソース機器は、図17のソース機器からMACアドレス記録部24、MACアドレス検索処理部25及びMACアドレス比較処理部26を省略し、その代わりに図18のシンク機器と同様のMACアドレス検索事前通知受信処理部63、VPNクライアント部及びMACアドレス送信部を追加した構成になっている。

【0132】

図26はシンク機器の第5の実施形態の内部構成を示すブロック図である。図26のシンク機器は、図18のシンク機器からMACアドレス検索事前通知受信処理部63、VPNクライアント部及びMACアドレス送信部を省略し、その代わりに図17のソース機器と同様のMACアドレス記録部24、MACアドレス検索処理部25、MACアドレス比較処理部26及びMACアドレス検索事前通知処理部62を追加した構成になっている。

【0133】

図27はソース機器とシンク機器が物理的に同一のセグメントに存在する場合における第5の実施形態の処理手順を示すシーケンス図である。なお、図27の処理を開始する前提として、シンク機器とソース機器との間でDTCP認証・鍵交換処理が行われており、シンク機器はソース機器のMACアドレスを事前に取得しているものとする。

【0134】

まず、シンク機器はソース機器にMACアドレス検索事前通知を送信する（ステップS71）とともに、ソース機器のIPアドレスからMACアドレス検索を行う（ステップS72）。

【0135】

ソース機器は、シンク機器からのMACアドレス検索を受信すると（ステップS73）、自機器のMACアドレスをシンク機器に送信する（ステップS74）。

【0136】

シンク機器は、ソース機器から送信されたMACアドレスと事前に取得しているソース機器のMACアドレスとが一致するか否かを比較判定し（ステップS75）、両者が一致すれば、ソース機器からのコンテンツを受信する（ステップS76）。

【0137】

ソース機器は、シンク機器からのMACアドレス検索要求を受信したか否かを判定し（ステップS77）、受信した場合にはコンテンツの受信を継続して行い（ステップS78）、受信しなかった場合には所定のエラー処理を行って、コンテンツの受信を中止する。

【0138】

図28はソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第5の実施形態の処理手順を示すシーケンス図である。この場合、シンク機器と同一のセグメントにはソース機器は接続されていないため、シンク機器から上位のプロトコルで送信されたMACアドレス検索事前通知はソース機器に届くが（ステップS81）、ソース機器のIPアドレスからMACアドレスを検索しようとしても（ステップS82）、VPNサーバ機器が代理で応答してしまう（ステップS83）。

【0139】

仮にVPNサーバ機器のMACアドレスがソース機器のMACアドレスと同一であったとすると、シンク機器でのMACアドレス比較結果は一致し（ステップS84）、ソース機器はシンク機器にコンテンツを送信してしまう（ステップS85）。

【0140】

ところが、ソース機器はIPアドレスからのMACアドレス検索を受信していないため（ステップS86）、コンテンツの送信を中止する（ステップS87）。

【0141】

このように、第5の実施形態では、シンク機器と同一セグメントに接続されているVPNサーバ機器がソース機器と同一のMACアドレスであっても、ソース機器が同一セグメントに接続されていない限り、コンテンツの送信を確実に中止できる。

【0142】

（第6の実施形態）

第6の実施形態は、ソース機器がシンク機器からのMACアドレス検索事前通知を受けると、それに対する応答をシンク機器に送信するようにしたものである。

【0143】

図29はソース機器の第6の実施形態の内部構成を示すブロック図である。図29のソース機器は、図25のソース機器の構成に加えて、MACアドレス検索事前通知応答をシンク機器に送信する制御を行うMACアドレス検索事前通知応答処理部65を有する。

【0144】

図30はシンク機器の第6の実施形態の内部構成を示すブロック図である。図30のシンク機器は、図26のシンク機器の構成に加えて、ソース機器からのMACアドレス検索事前通知応答を受信する制御を行うMACアドレス検索事前通知応答受信処理部64を有する。

【0145】

図31はソース機器とシンク機器が物理的に同一のセグメントに存在する場合における第6の実施形態の処理手順を示すシーケンス図である。なお、図31の処理を開始する前提として、シンク機器とソース機器との間でDTCP認証・鍵交換処理が行われており、シンク機器はソース機器のMACアドレスを事前に取得しているものとする。

【0146】

以下では、図27と異なる処理を中心に説明する。ソース機器は、シンク機器

からのMACアドレス検索事前通知を受信すると（ステップS 9 1）、それに対する応答（MACアドレス検索事前通知応答）をシンク機器に送信する（ステップS 9 3）。

【0147】

シンク機器は、ソース機器からのMACアドレス検索事前通知応答を受信し（ステップS 9 5）、MACアドレスの比較処理を行う（ステップS 9 6）。次に、シンク機器はMACアドレス検索事前通知応答を受信したか否かを判定し（ステップS 9 7）、受信した場合にはソース機器からのコンテンツ送信を受ける（ステップS 9 8）。

【0148】

図3 2はソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第6の実施形態の処理手順を示すシーケンス図である。シンク機器は上位のプロトコルを用いてMACアドレス検索事前通知をソース機器に送信するため（ステップS 10 1）、この通知をソース機器は受信できるが、シンク機器がソース機器のIPアドレスからMACアドレス検索を行うと（ステップS 10 2）、シンク機器と同一セグメントに位置するVPNサーバ機器がMACアドレスを代理で応答する（ステップS 10 3）。

【0149】

VPNサーバ機器のMACアドレスがソース機器のMACアドレスと同一であれば、シンク機器でのMACアドレス比較結果は一致するが（ステップS 10 4）、シンク機器はソース機器からのMACアドレス検索事前通知応答を受信していないため（ステップS 10 5）、ソース機器に対してコンテンツ送信の中止を依頼し（ステップS 10 6）、これにより、ソース機器はコンテンツ送信を中止する（ステップS 10 7）。

【0150】

このように、第6の実施形態では、シンク機器からソース機器に送信したMACアドレス検索事前通知に対する応答がシンク機器で受信された場合のみ、コンテンツ送信を行うようにしたため、シンク機器とソース機器とが同一のセグメントに位置する場合のみコンテンツ送信を行うことができる。

【0151】**【発明の効果】**

以上詳細に説明したように、本発明によれば、機器識別情報検索手段で検索された機器識別情報と機器識別情報登録手段に登録されている機器識別情報とが一致する場合のみ、対応する受信装置へのコンテンツの送信を許可するため、限られた受信装置のみにコンテンツを提供でき、コンテンツの不正受信を防止できる。

【0152】

これにより、同じサブネットの複数の受信装置のうち、物理的に同一のサブネットに接続されている受信装置と、仮想的に同一のサブネットに接続されている受信装置とを区別して、前者と後方でコンテンツの配布条件を変えることができる。

【0153】

また、本発明によれば、送信装置からの機器時期別情報検索要求を受信装置が受信したか否かを確認することにより、送信装置と受信装置とが同一のセグメントに接続されているか否かを簡易かつ正確に判断できる。

【図面の簡単な説明】**【図1】**

本発明に係るコンテンツ送受信システムの第1の実施形態の概略構成を示すブロック図。

【図2】

ソース機器Aの内部構成の一例を示すブロック図。

【図3】

MACアドレステーブルの構造を示す図。

【図4】

シンク機器B、Cの内部構成の一例を示すブロック図。

【図5】

本実施形態の通信システムの処理手順を示す図。

【図6】

本実施形態の通信システムの処理手順を示す図。

【図 7】

ソース機器 A の処理手順を示す図。

【図 8】

ソース機器とシンク機器との間に VPN サーバ機器が接続されているコンテンツ送受信システムの概略構成を示すブロック図。

【図 9】

本発明に係るコンテンツ送受信システムの第 2 の実施形態の概略構成を示すブロック図。

【図 10】

VPN サーバ機器 F と VPN クライアント機器 G が二つのネットワークをトンネリングするコンテンツ送受信システムのブロック構成を示す図。

【図 11】

図 10 で示したコンテンツ送受信システムの形態におけるソース機器の内部構成を示すブロック図。

【図 12】

図 10 で示したコンテンツ送受信システムの形態におけるシンク機器の内部構成を示すブロック図。

【図 13】

シンク機器の内部で MAC アドレスの比較を行う場合のソース機器の内部構成を示すブロック図。

【図 14】

シンク機器の内部で MAC アドレスの比較を行う場合のシンク機器の内部構成を示すブロック図。

【図 15】

VPN 機器の接続形態の種類を示す図。

【図 16】

本発明に係るコンテンツ送受信システムの第 3 の実施形態の概略構成を示すブロック図。

【図 17】

第3の実施形態におけるソース機器A15の内部構成を示すブロック図。

【図 18】

第3の実施形態におけるシンク機器B11, C12の内部構成を示すブロック図。

【図 19】

第3の実施形態の処理手順を示すシーケンス図。

【図 20】

ソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第3の実施形態の処理手順を示すシーケンス図。

【図 21】

ソース機器の第4の実施形態の内部構成を示すブロック図。

【図 22】

シンク機器の第4の実施形態の内部構成を示すブロック図。

【図 23】

第4の実施形態の処理手順を示すシーケンス図。

【図 24】

ソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第4の実施形態の処理手順を示すシーケンス図。

【図 25】

ソース機器の第5の実施形態の内部構成を示すブロック図。

【図 26】

シンク機器の第5の実施形態の内部構成を示すブロック図。

【図 27】

ソース機器とシンク機器が物理的に同一のセグメントに存在する場合における第5の実施形態の処理手順を示すシーケンス図。

【図 28】

ソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第5の実施形態の処理手順を示すシーケンス図。

【図 29】

ソース機器の第6の実施形態の内部構成を示すブロック図。

【図30】

シンク機器の第6の実施形態の内部構成を示すブロック図。

【図31】

ソース機器とシンク機器が物理的に同一のセグメントに存在する場合における第6の実施形態の処理手順を示すシーケンス図。

【図32】

ソース機器とシンク機器が物理的に同一のセグメントに存在しない場合における第6の実施形態の処理手順を示すシーケンス図。

【図33】

送信装置と受信装置を備えた従来のネットワークシステムの全体構成を示すブロック図。

【図34】

インターネットセグメントA、Bにそれぞれ別個のシンク機器が接続されているネットワークシステムの全体構成を示すブロック図。

【図35】

ソース機器とシンク機器のネットワークアドレスが同一か否かを判別する処理手順を示すフローチャート。

【図36】

VPNを使ったネットワーク構成の一例を示す図。

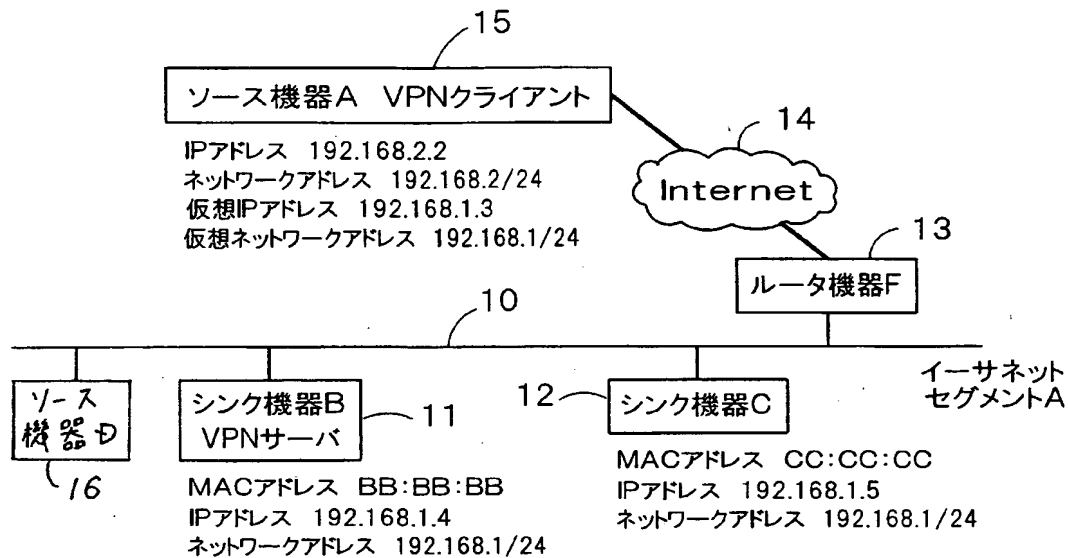
【符号の説明】

- 10 イーサネットセグメントA
- 11 シンク機器B
- 12 シンク機器C
- 13 ルータ機器F
- 14 インターネット
- 15 ソース機器A
- 21 ネットワークインタフェース部
- 22 通信処理部

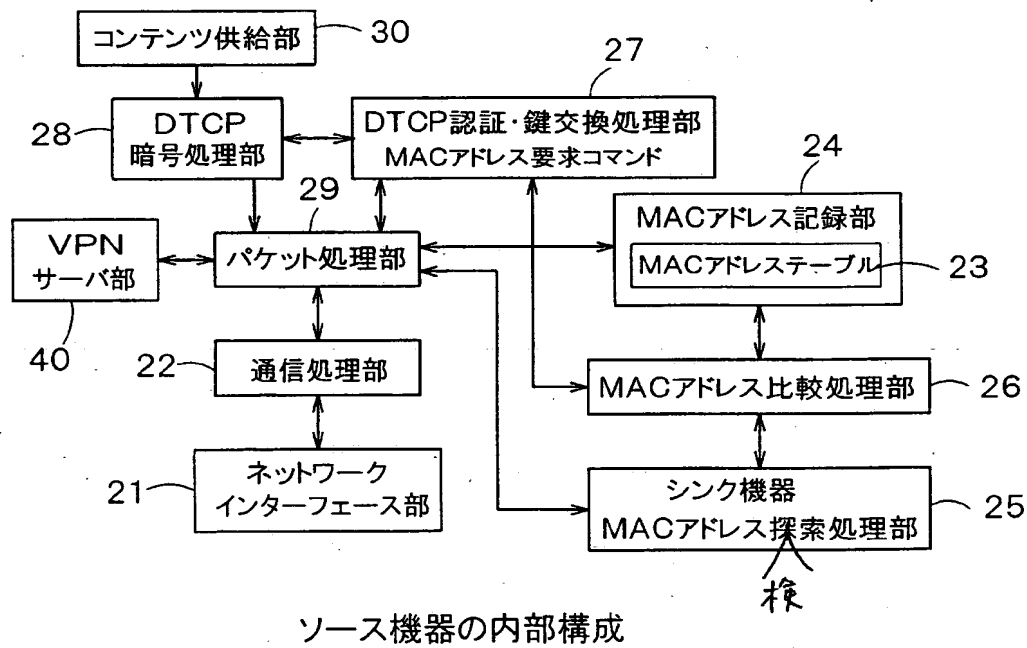
- 2 3 MACアドレステーブル
- 2 4 MACアドレス記録部
- 2 5 シンク機器MACアドレス検索処理部
- 2 6 MACアドレス比較処理部
- 2 7 DTCP認証・鍵交換処理部
- 2 8 DTCP暗号処理部
- 2 9 パケット処理部
- 3 0 コンテンツ供給部
- 3 1 ネットワークインタフェース部
- 3 2 通信処理部
- 3 3 MACアドレス送信部
- 3 4 VPNクライアント部
- 3 5 DTCP認証・鍵交換処理部
- 3 6 DTCP暗号処理部
- 3 7 パケット処理部
- 3 8 コンテンツ処理部
- 6 2 MACアドレス検索事前通知処理部
- 6 3 MACアドレス検索事前通知受信処理部
- 6 4 MACアドレス検索事前通知応答受信処理部
- 6 5 MACアドレス検索事前通知応答処理部

【書類名】 図面

【図 1】



【図 2】

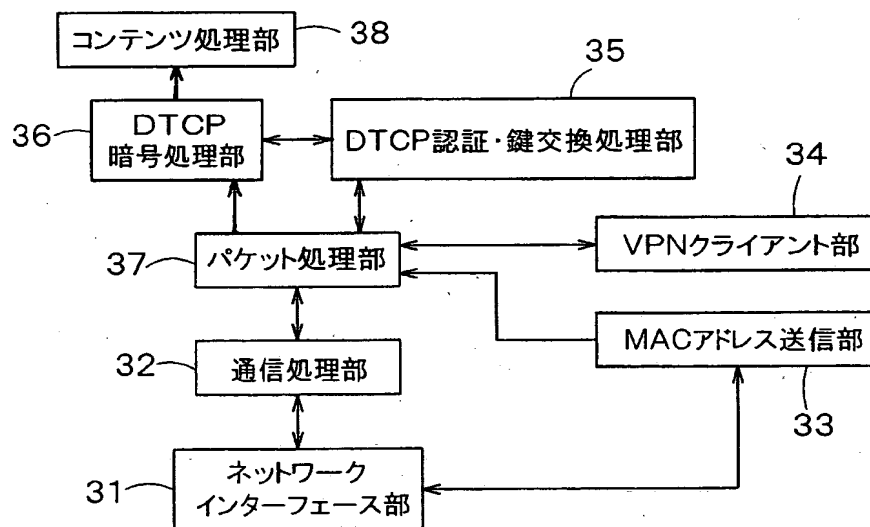


【図 3】

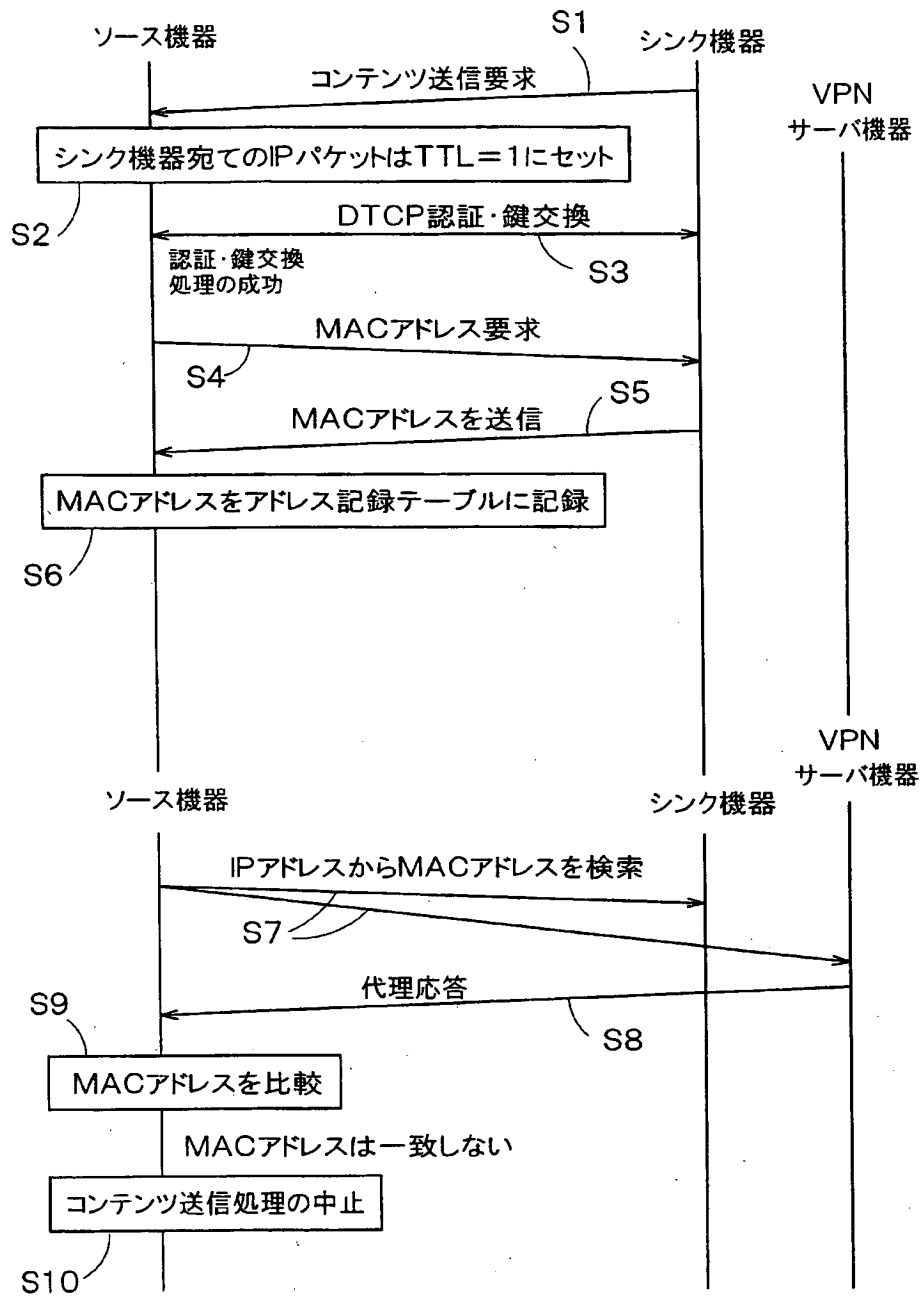
MACアドレステーブル

	IPアドレス	MACアドレス	デバイスID
シンク機器B	192.168.1.3	BB:BB:BB	B1
シンク機器C	192.168.1.5	CC:CC:CC	C1
シンク機器X	192.168.78	XX:XX:XX	X1
....			

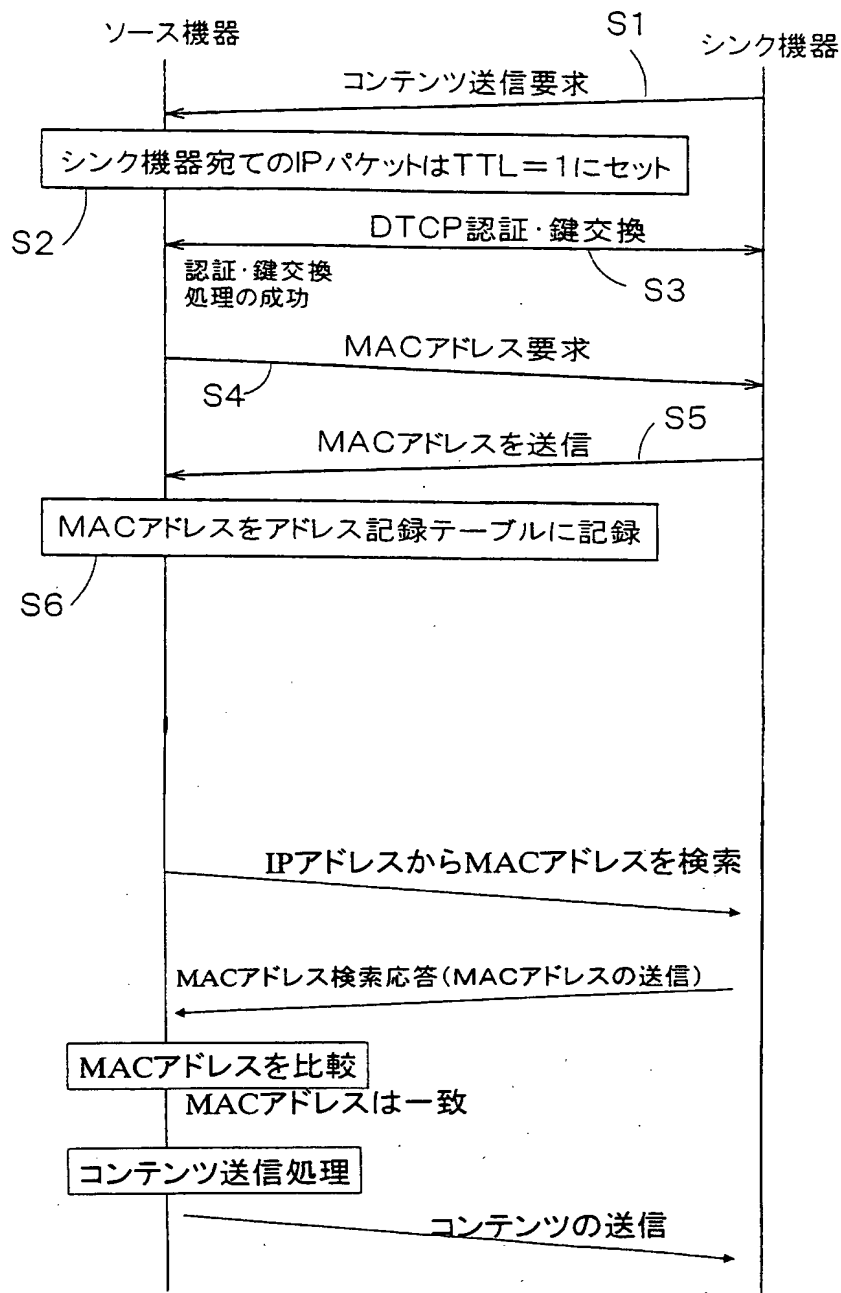
【図 4】

シンク機器の内部構成

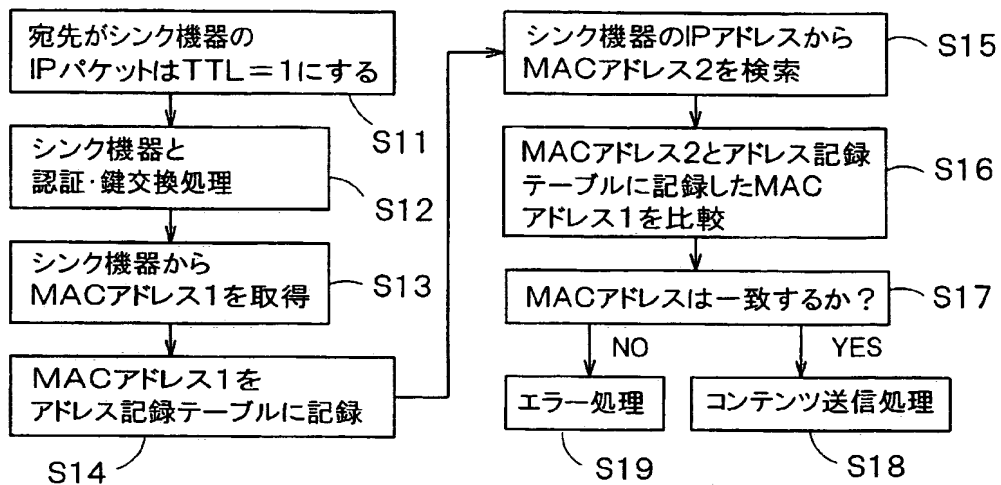
【図 5】



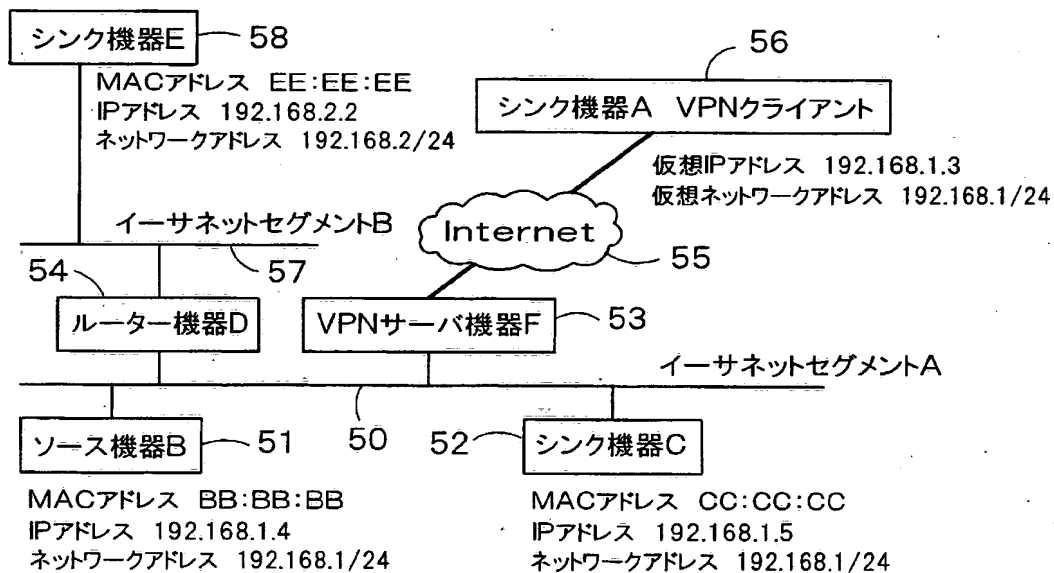
【図 6】



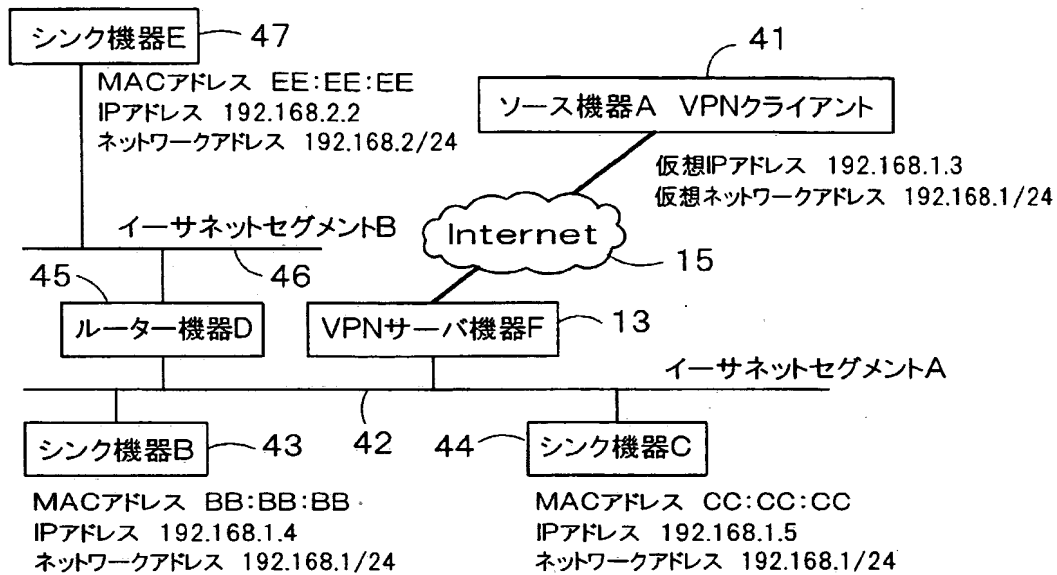
【図 7】



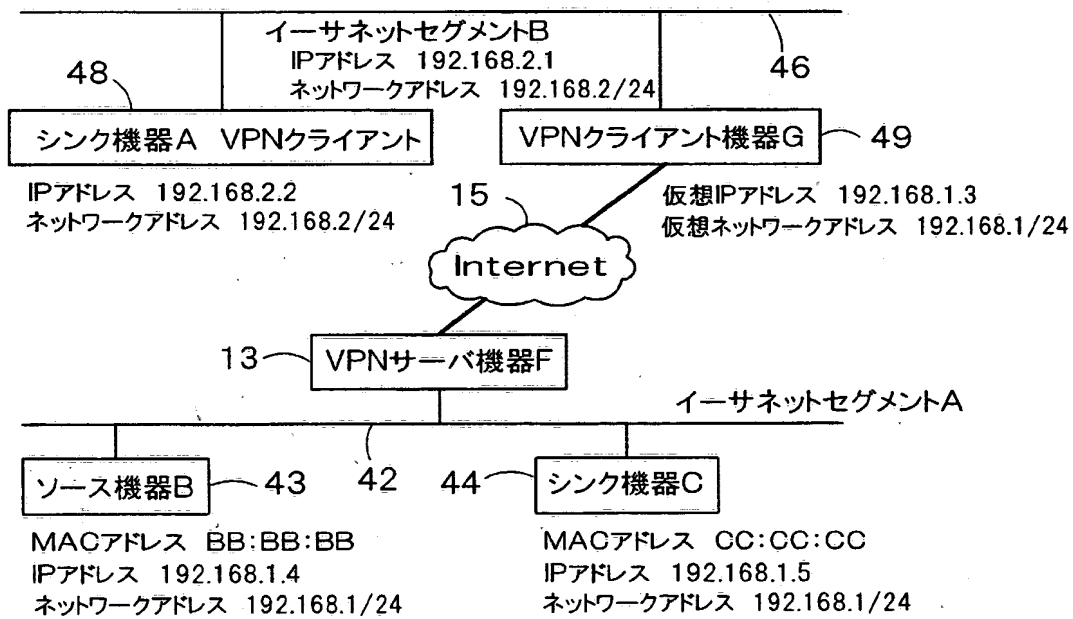
【図 8】



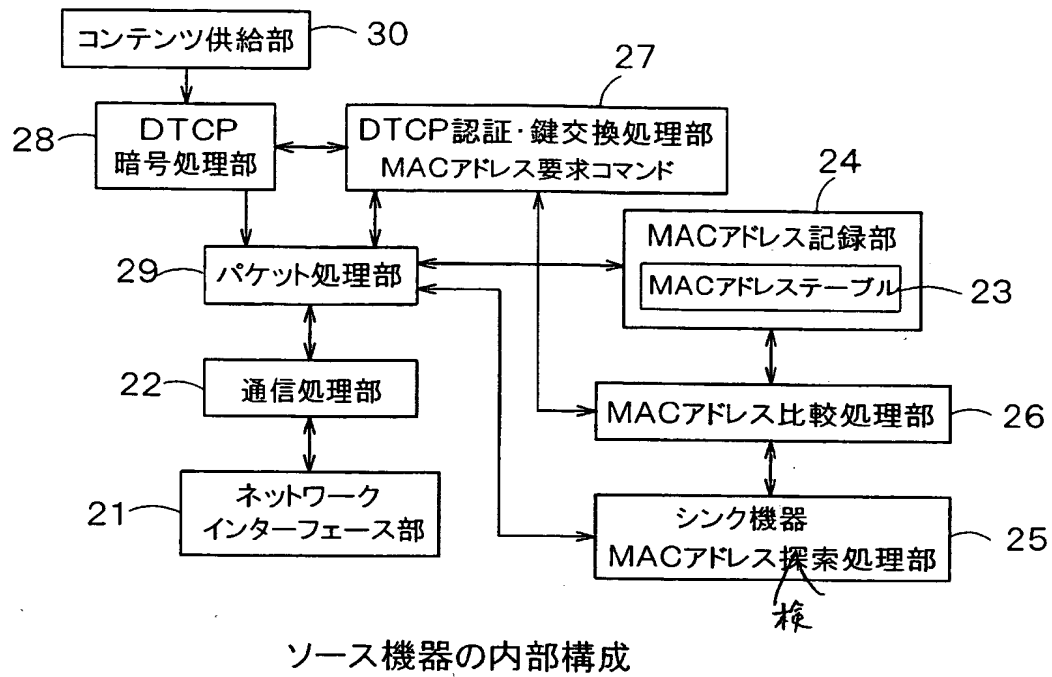
【図 9】



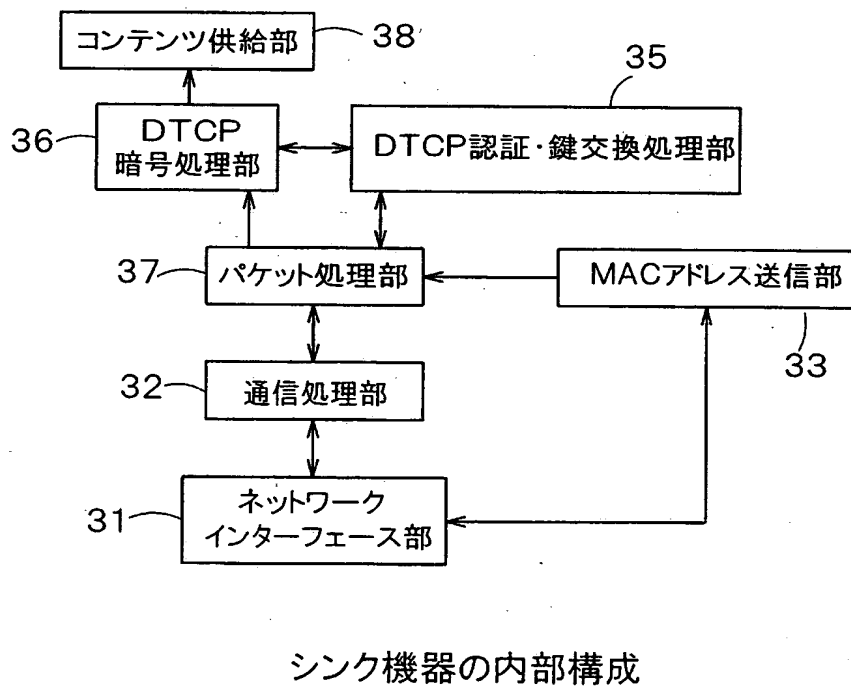
【図 10】



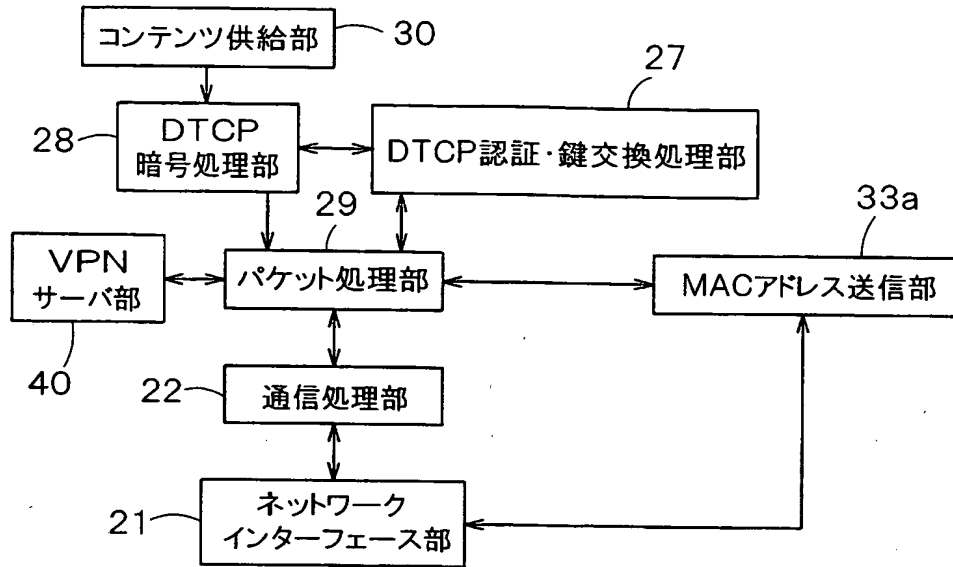
【図 11】



【図 12】

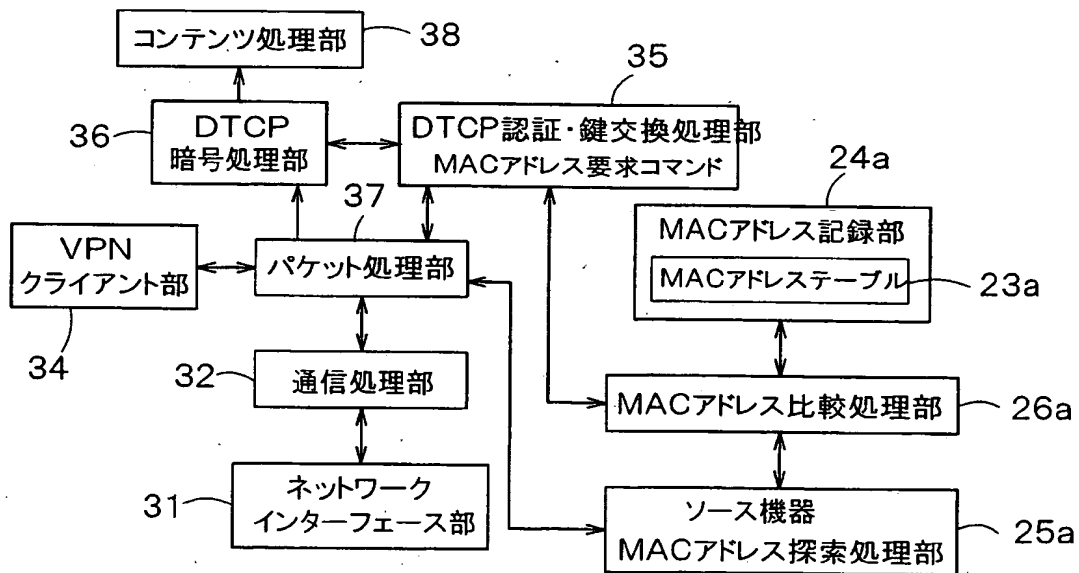


【図 13】



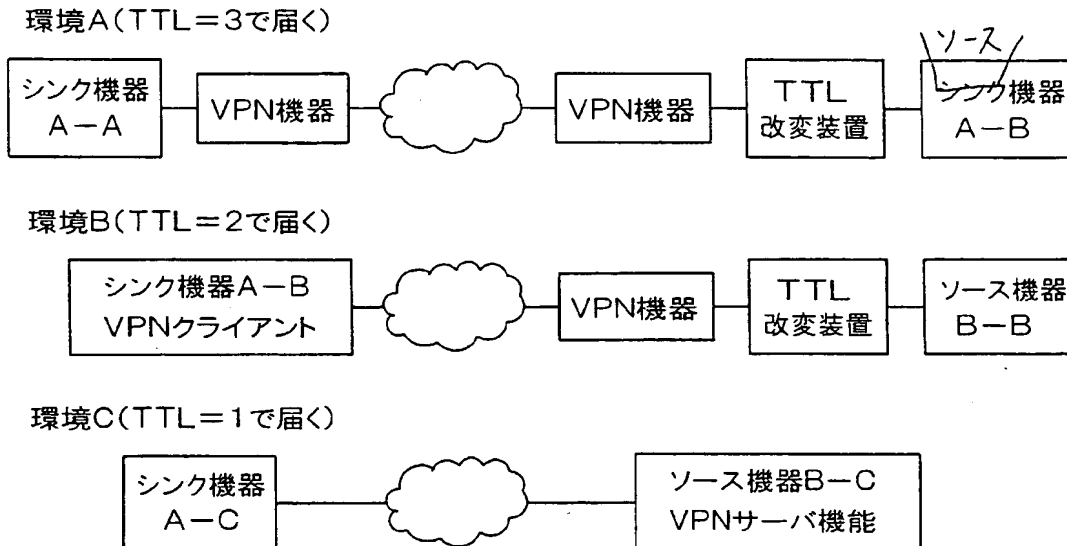
ソース機器の内部構成

【図 14】



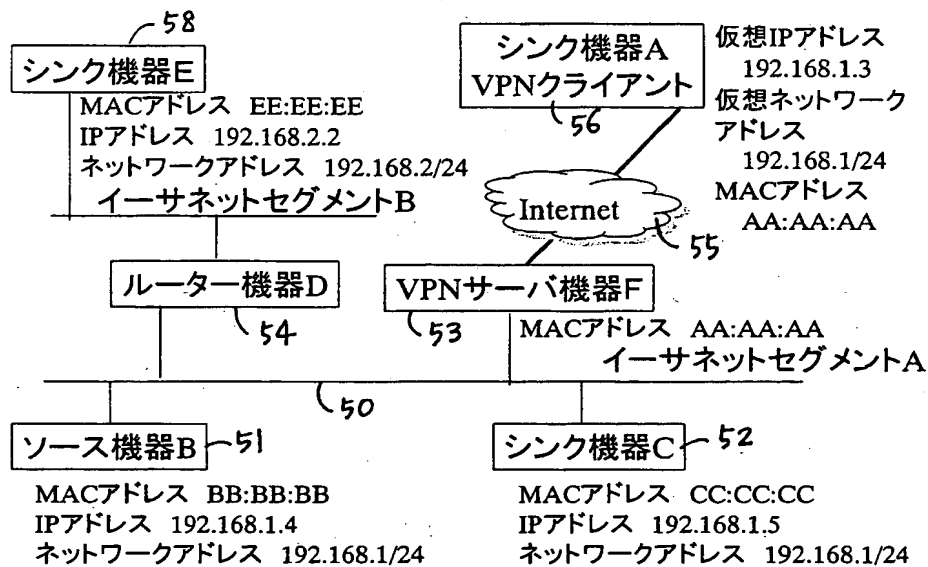
シンク機器の内部構成

【図15】

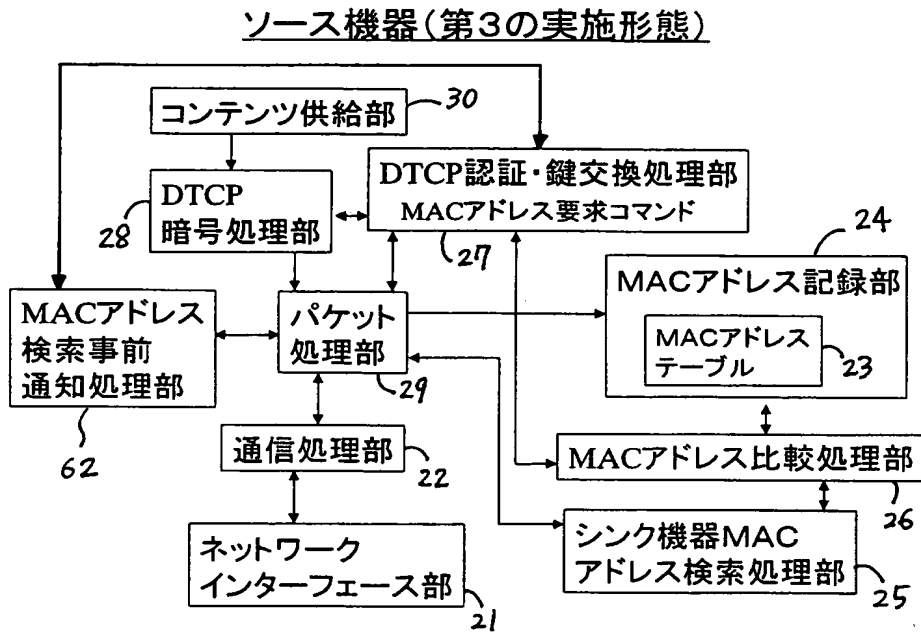


【図16】

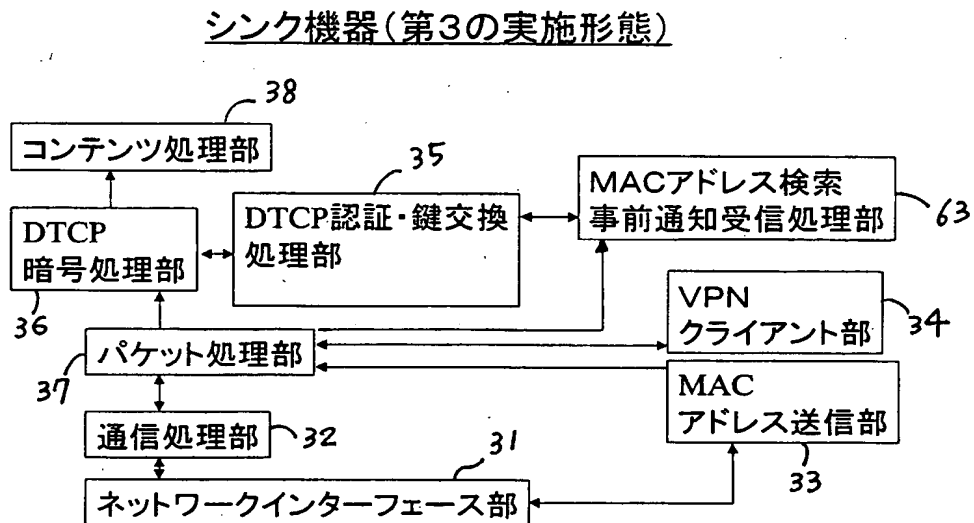
全体システム図(第3の実施形態)



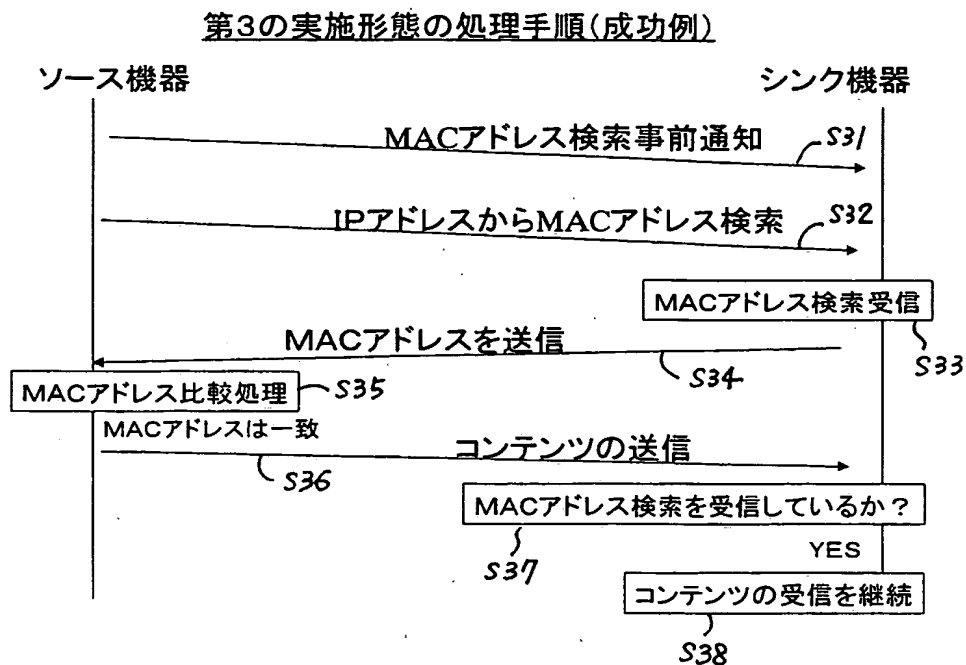
【図 17】



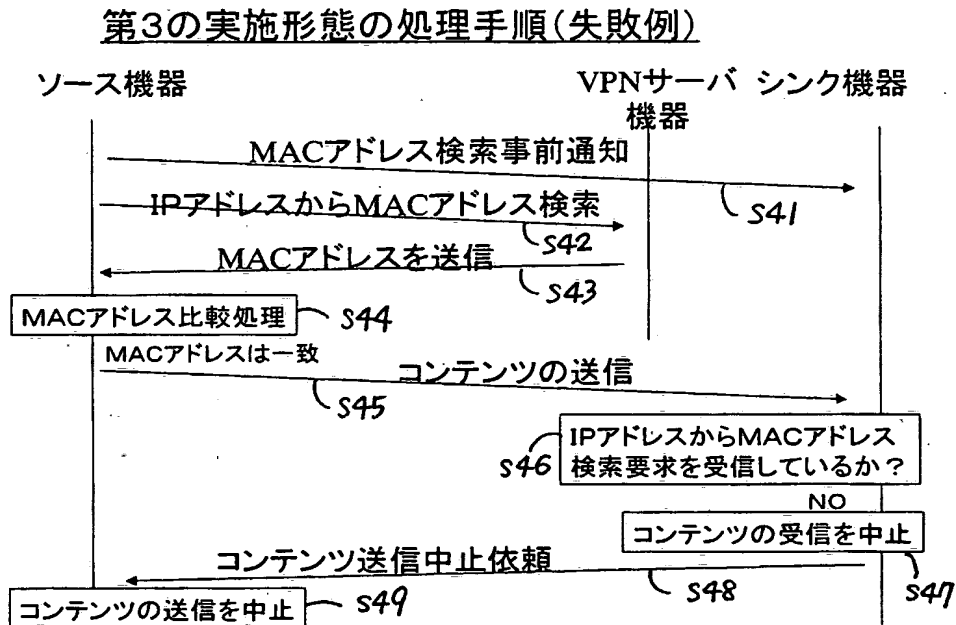
【図 18】



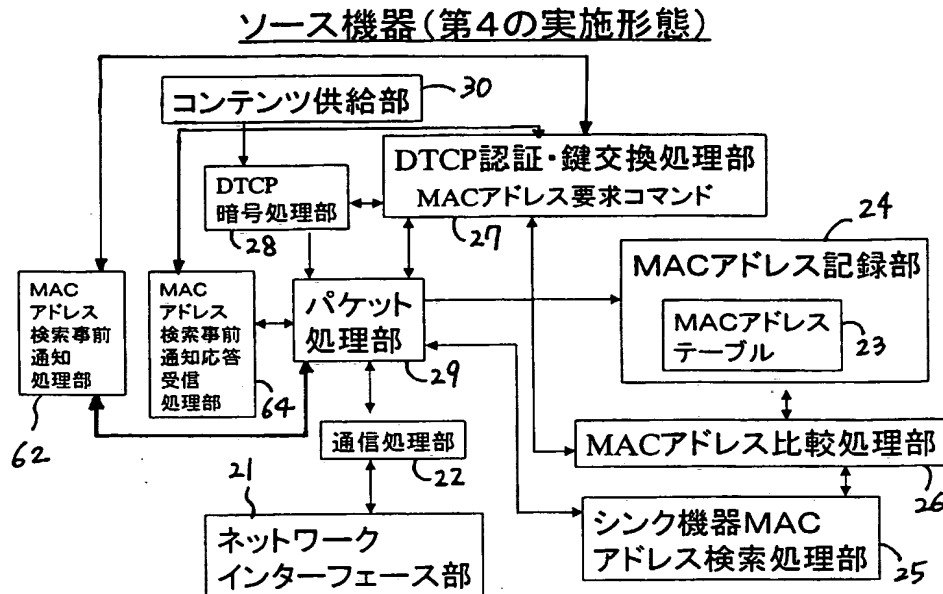
【図 19】



【図 20】

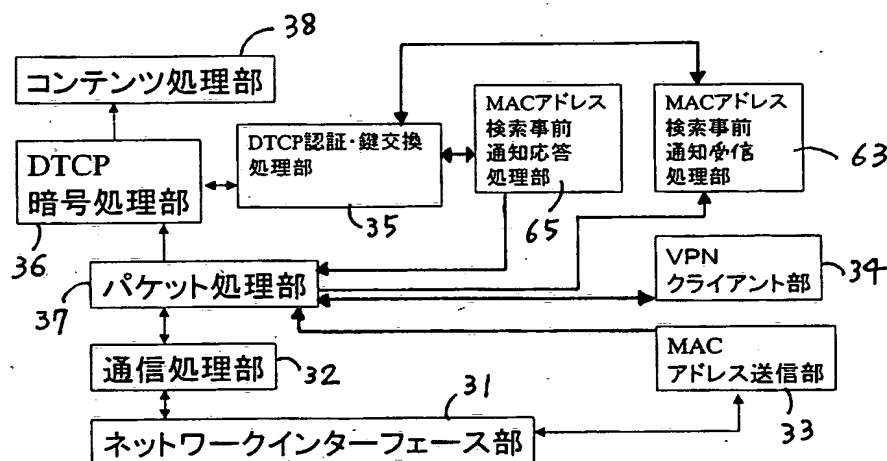


【図 21】



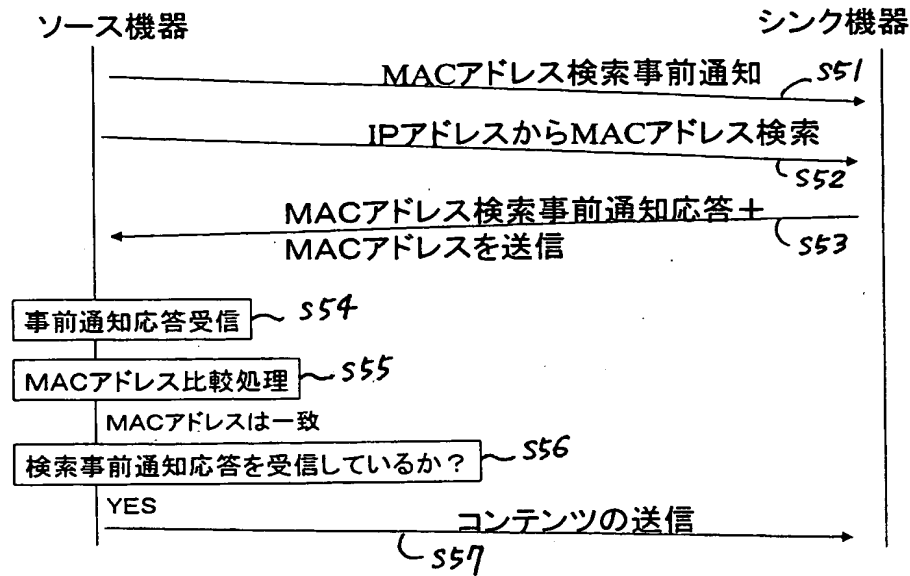
【図 22】

シンク機器(第4の実施形態)



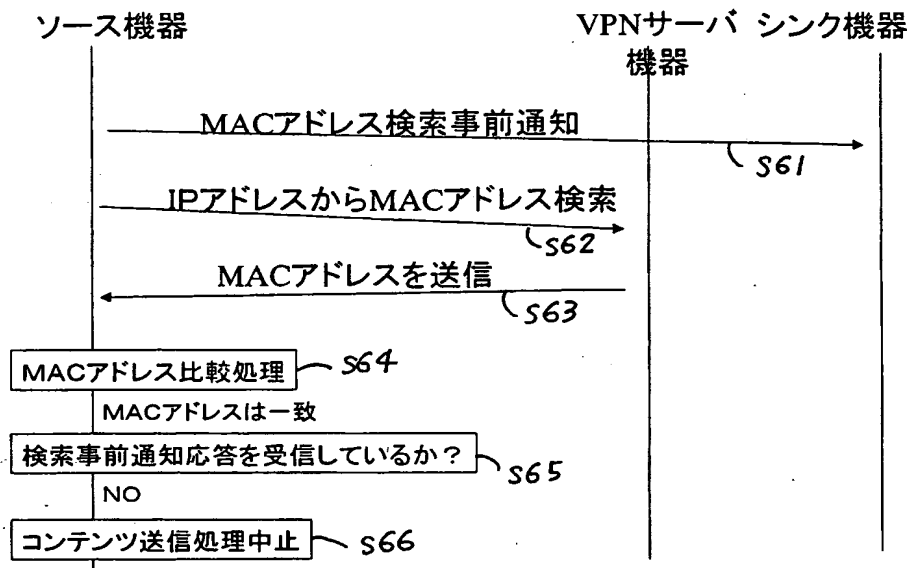
【図 2 3】

第4の実施形態の処理手順(成功例)



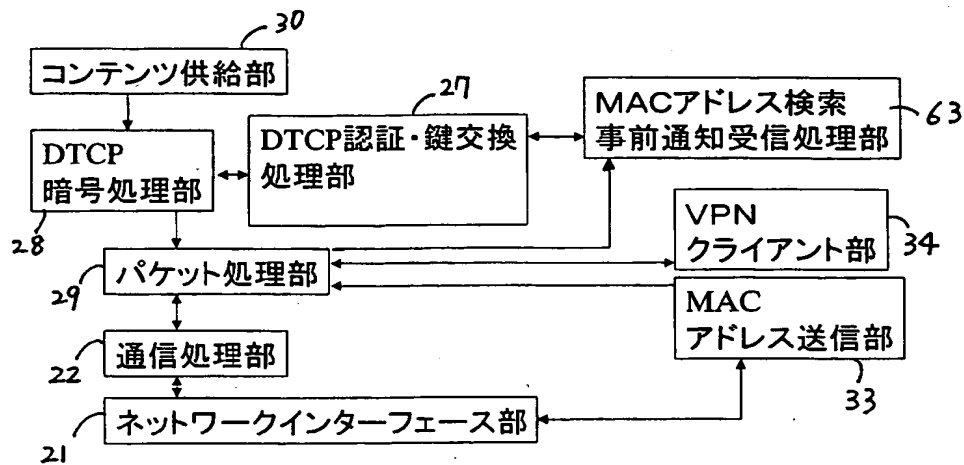
【図 2 4】

第4の実施形態の処理手順(失敗例)



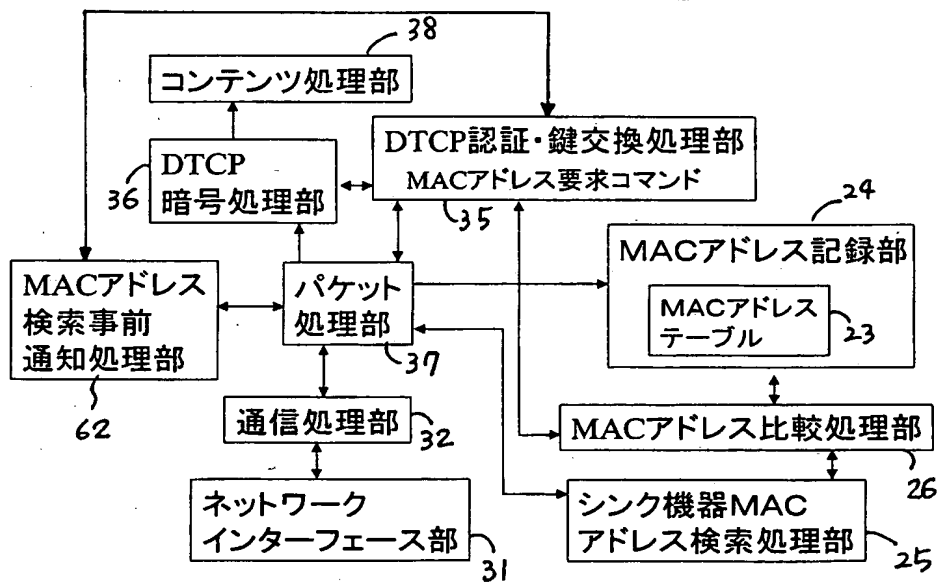
【図 25】

ソース機器(第5の実施形態)

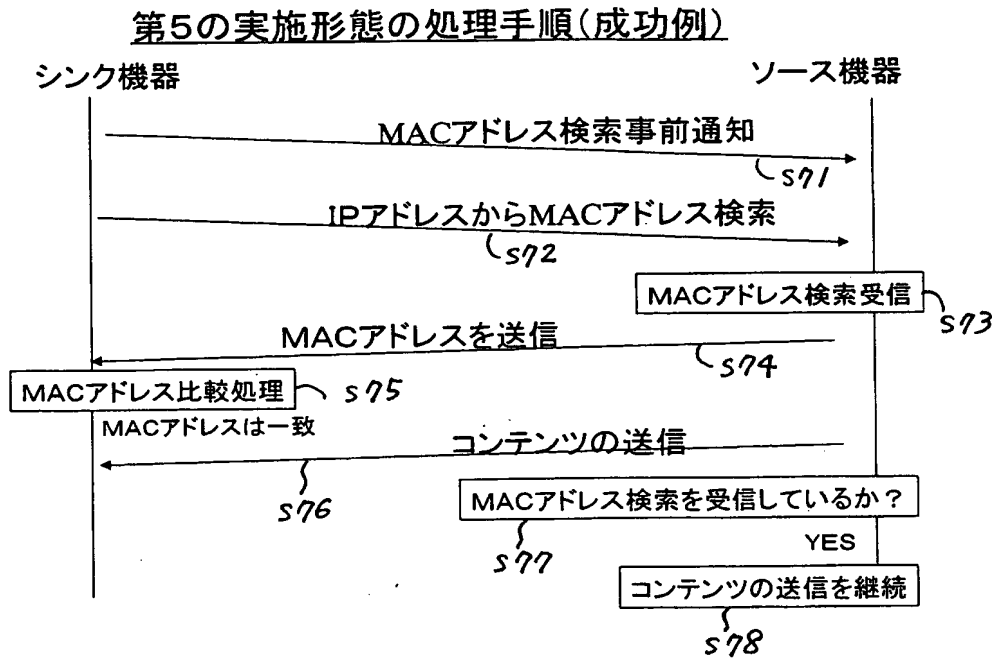


【図 26】

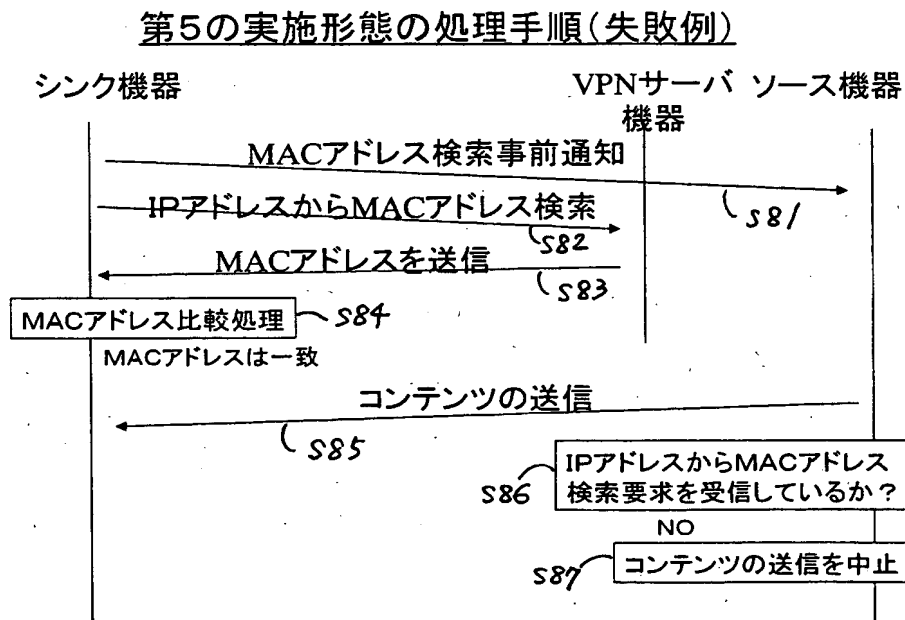
シンク機器(第5の実施形態)



【図 27】

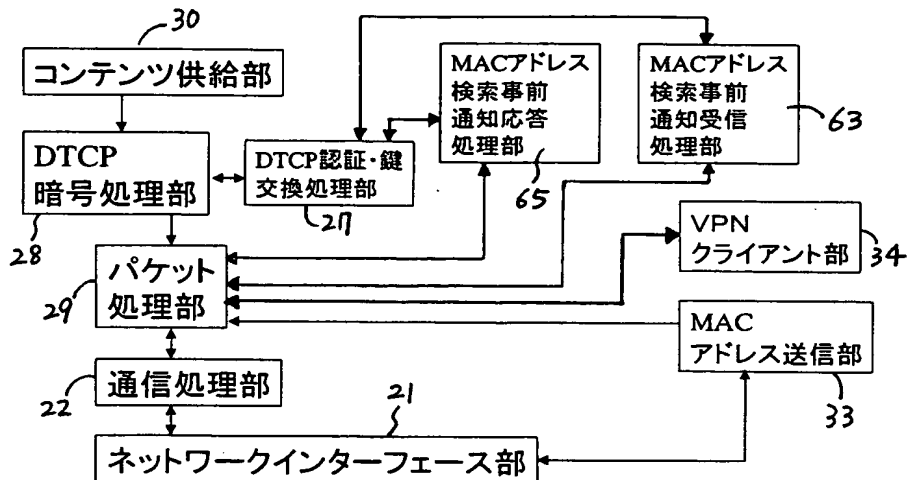


【図 28】



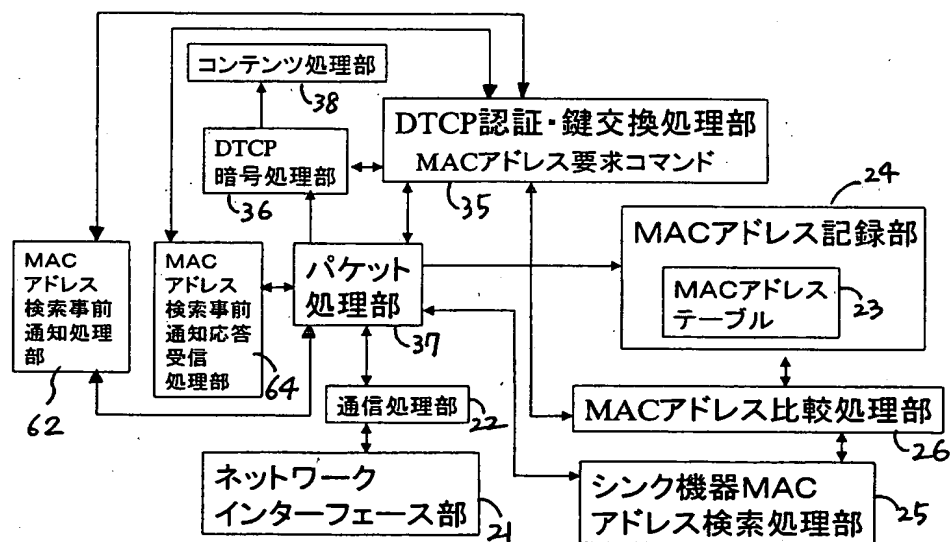
【図 29】

ソース機器(第6の実施形態)

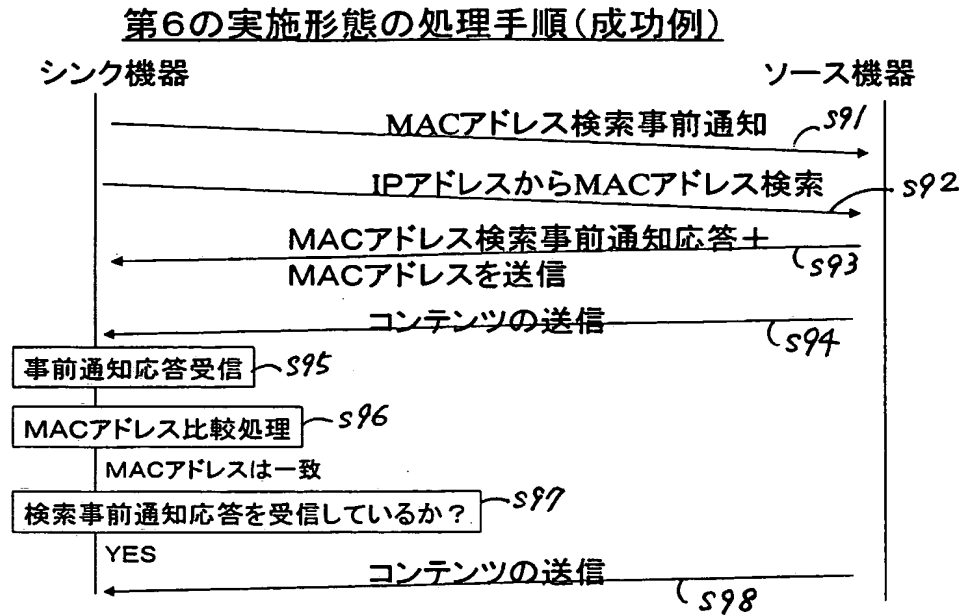


【図 30】

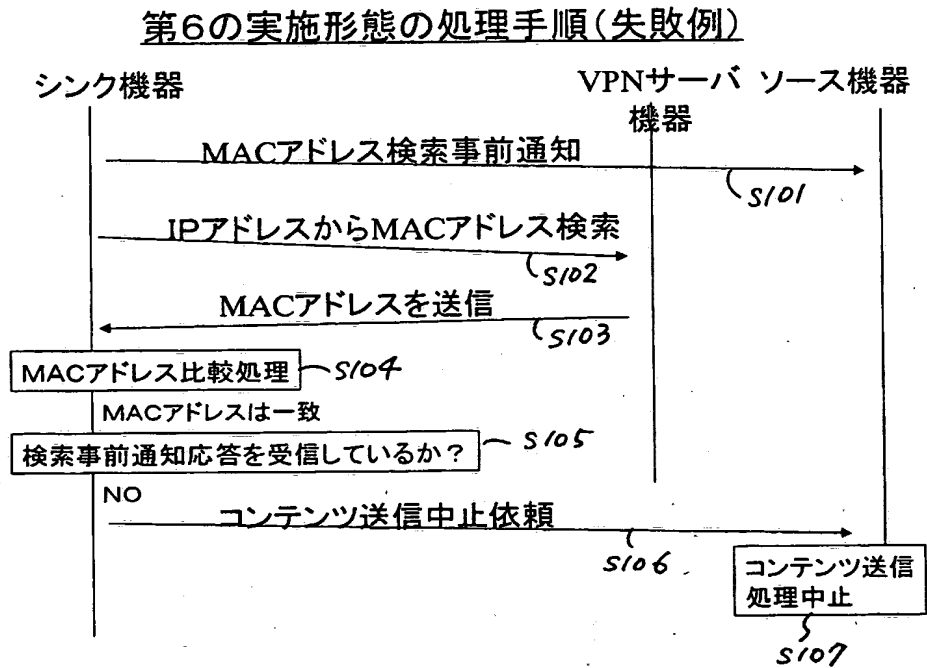
シンク機器(第6の実施形態)



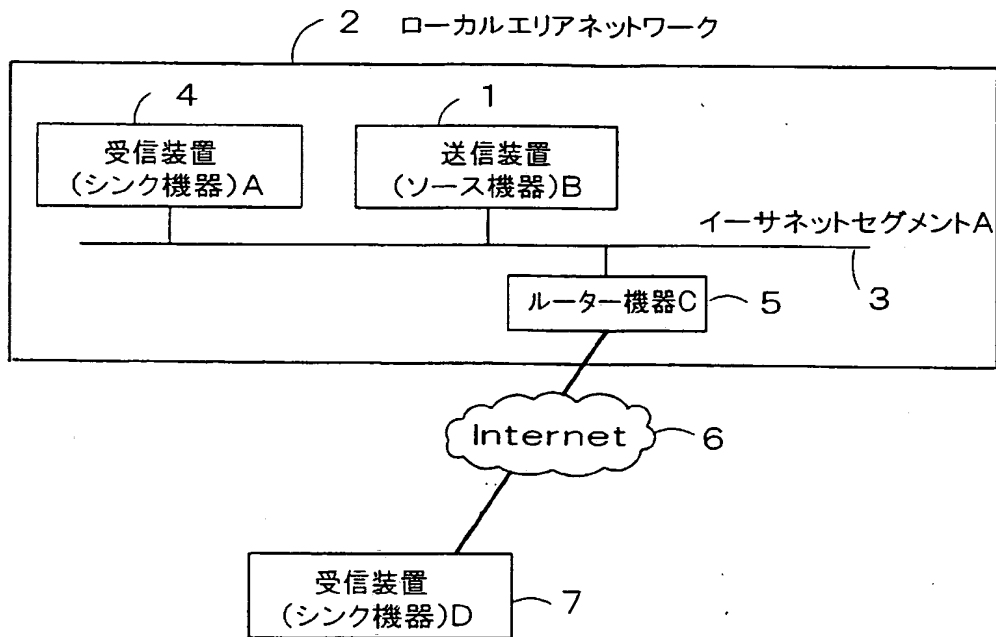
【図 3 1】



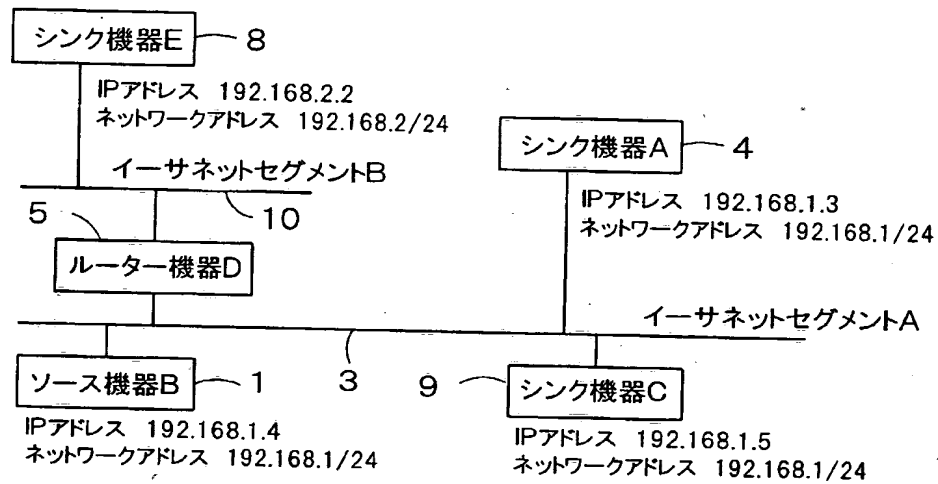
【図 3 2】



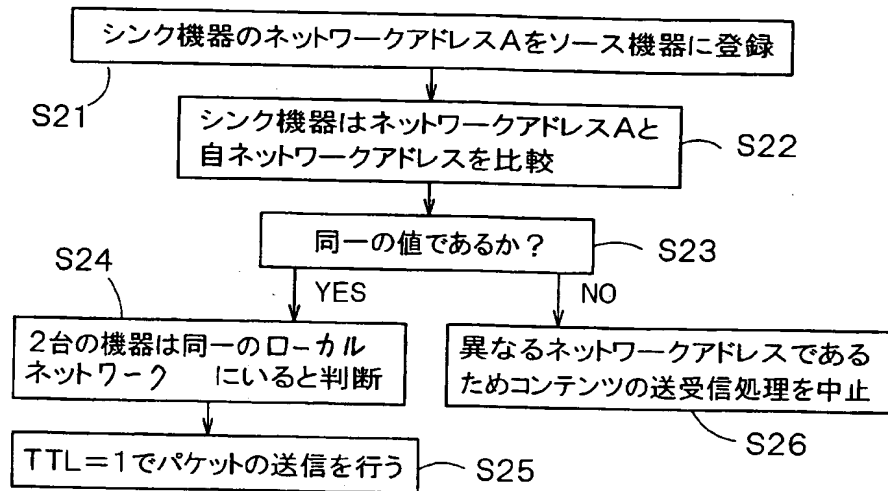
【図 3 3】



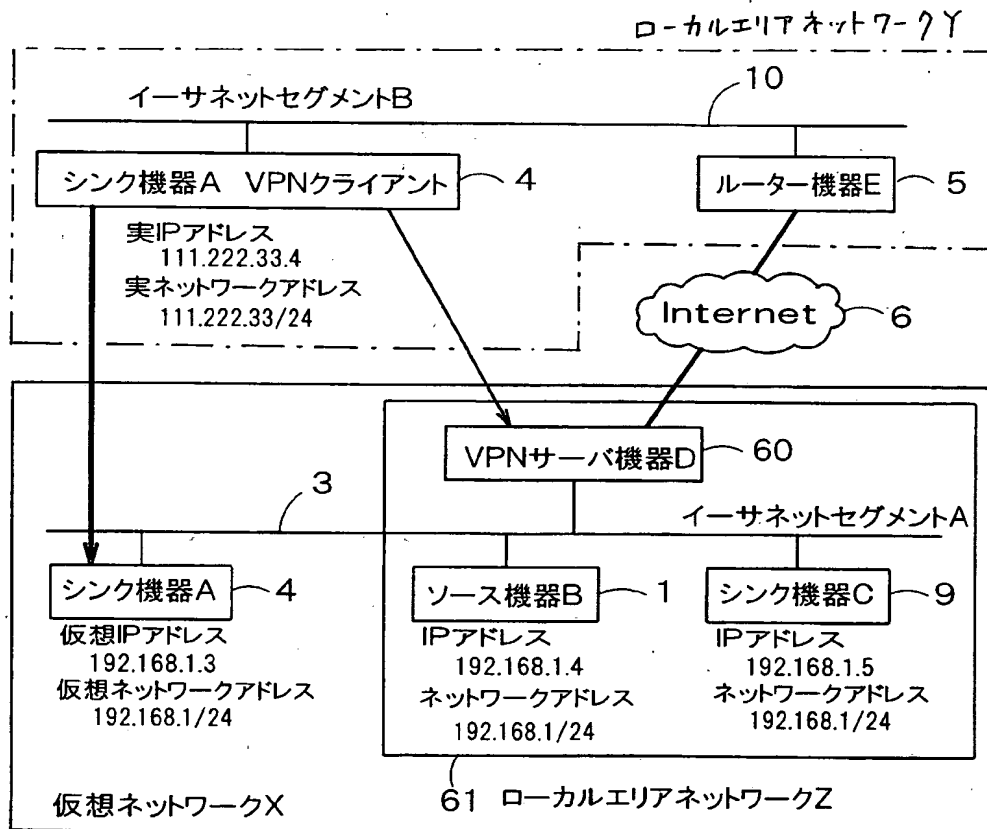
【図 3 4】



【図 3 5】



【図 3 6】



【書類名】 要約書

【要約】

【課題】 限られた受信装置だけにコンテンツを送信可能にする。

【解決手段】 本発明に係るコンテンツ送受信システムは、イーサネットセグメントA10に接続されるシンク機器B11、シンク機器B12及びルータ機器F13と、ルータ機器F13にインターネット14を介して接続されるソース機器A15とを有する。ソース機器B51は同一イーサネットセグメントA10に接続されているシンク機器のみにコンテンツの送受信を許可するため、例えばVPNサーバ機器F53を介して接続されるシンク機器等へのコンテンツの送受信を確実に禁止できる。

【選択図】 図1

認定・付加情報

特許出願の番号	特願 2002-357168
受付番号	50201862421
書類名	特許願
担当官	第七担当上席 0096
作成日	平成 14 年 12 月 12 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000003078
【住所又は居所】	東京都港区芝浦一丁目 1 番 1 号
【氏名又は名称】	株式会社東芝

【代理人】

申請人	
【識別番号】	100075812
【住所又は居所】	東京都千代田区丸の内 3-2-3 協和特許法律事務所
【氏名又は名称】	吉武 賢次

【選任した代理人】

【識別番号】	100088889
【住所又は居所】	東京都千代田区丸の内 3 丁目 2 番 3 号 協和特許法律事務所
【氏名又は名称】	橘谷 英俊

【選任した代理人】

【識別番号】	100082991
【住所又は居所】	東京都千代田区丸の内 3 丁目 2 番 3 号 富士ビル 協和特許法律事務所
【氏名又は名称】	佐藤 泰和

【選任した代理人】

【識別番号】	100096921
【住所又は居所】	東京都千代田区丸の内 3-2-3 富士ビル 3 階 協和特許法律事務所
【氏名又は名称】	吉元 弘

【選任した代理人】

【識別番号】	100103263
【住所又は居所】	東京都千代田区丸の内 3 丁目 2 番 3 号 協和特許法律事務所

次頁有

認定・付加情報（続き）

【氏名又は名称】 川崎 康

次頁無

特願 2002-357168

出願人履歴情報

識別番号

[000003078]

1. 変更年月日 2001年 7月 2日
[変更理由] 住所変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝
2. 変更年月日 2003年 5月 9日
[変更理由] 名称変更
住所変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝